Titre: Title:	Concepts d'analyse de la vulnérabilité des infrastructures essentielles - prise en compte de la cybernétique
Auteur: Author:	Frédéric Petit
Date:	2009
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Petit, F. (2009). Concepts d'analyse de la vulnérabilité des infrastructures essentielles - prise en compte de la cybernétique [Thèse de doctorat, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/8291/

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/8291/
Directeurs de recherche: Advisors:	
Programme: Program:	Non spécifié

UNIVERSITÉ DE MONTRÉAL

CONCEPTS D'ANALYSE DE LA VULNÉRABILITÉ DES INFRASTRUCTURES ESSENTIELLES - PRISE EN COMPTE DE LA CYBERNÉTIQUE

FRÉDÉRIC PETIT
DÉPARTEMENT DES GÉNIES CIVIL, GÉOLOGIQUE ET DES MINES
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

THÈSE PRÉSENTÉE EN VUE DE L'OBTENTION
DU DIPLÔME DE PHILOSOPHIAE DOCTOR (Ph. D.)
(GÉNIE CIVIL)
AVRIL 2009

Your file Votre référence
ISBN: 978-0-494-49424-0
Our file Notre référence
ISBN: 978-0-494-49424-0

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Cette thèse intitulée :

CONCEPTS D'ANALYSE DE LA VULNÉRABILITÉ DES INFRASTRUCTURES ESSENTIELLES - PRISE EN COMPTE DE LA CYBERNÉTIQUE

Présentée par : PETIT Frédéric

en vue de l'obtention du diplôme de : Philosophiae Doctor

a été dûment acceptée par le jury d'examen constitué de :

M. BOURGAULT Mario, Ph.D., président

M. ROBERT Benoît, Ph.D., membre et directeur de recherche

M. MARCHE Claude, D.Sc.A., membre et codirecteur de recherche

M. FISHER Ronald E., M.B.A, membre

M. VALLERAND Andrew L., Ph.D., membre

DÉDICACE

À loz anchin, lô Ptyou d'Noval, lô Lyon-n', lô Tâtyeu, lô molardî,

À Té, Pyapô, ké zhamé vâ lire mn ûvra,

À rlo d'la Hyôta Savoué è d'alyeu k'aron la pachinsa d'lo lire.

REMERCIEMENTS

Une thèse de doctorat est un travail de longue haleine qui ne peut se faire sans l'appui de nombreuses personnes. Il convient de les remercier, et ce, si possible, de manière originale. En fait, une analogie peut être faite entre les personnes qui m'ont soutenu durant les six ans qu'a duré mon doctorat et une équipe de rugby. Voici donc la composition de mon équipe :

Première ligne. La première ligne est sans aucun doute à la base de tout sur un terrain. Ils sont de tous les combats et participent à toutes les phases de conquête. Ces postes ne pouvaient revenir qu'à la famille Petit, le père et la mère à la pile, Titou au talon. Merci donc mes chers parents pour votre soutien de tous les instants et pour m'avoir permis de vivre mes délires et m'avoir supporté dans cette aventure. Merci frangin pour ton support, mais surtout pour m'avoir brassé lorsque je doutais de moi. Oui, je sais, talon, ce n'est pas vraiment ton poste habituel, mais tu as largement la caboche pour.

Deuxième ligne, les joueurs appréciés de tous, mais dont les actions sur le terrain ne sont pas toujours visibles. Doud's et Tom, ces postes vous reviennent de droit. Sans vous, je ne serais pas où j'en suis aujourd'hui. Merci les gars, je suis conscient de ce que je vous dois.

Troisième ligne, les joueurs de soutien dans le combat. Borissot au centre, Pap's et Jo sur les ailes. Quelle troisième ligne de rêve, prompte à l'exploit sportif et à l'exploit festif, les rois de la blagounette et du bon mot. Merci pour les instants de détente et de franche rigolade que vous m'avez apportés.

Demi de mêlée et entraîneur, deux pièces maîtresses de l'équipe. Ce poste et ce rôle ne peuvent revenir qu'à Benoît Robert, maître à jouer et maître à penser qui a réussi à

me conduire sur des terrains que je n'aurais sans doute jamais explorés sans lui. Le doctorat est une chose, mais il a réussi à faire que je me dépasse en tant que personne. Il ne m'a pas seulement encadré et conseillé pour ce travail, il m'a aussi enseigné le métier de chercheur et d'enseignant. Merci Benoît de m'avoir accordé ta confiance en me proposant d'effectuer un doctorat. Je pense que rien que pour cela, le bilan, que je peux faire de ces six ans d'étude, est largement positif. Finalement, je ne pourrai pas non plus oublier que tu m'as également appris l'humilité en me mettant quelques raclées mémorables au badminton.

Demi d'ouverture, Claude Marche. En acceptant d'être mon directeur puis mon codirecteur de recherche, vous m'avez permis de pouvoir entreprendre cette aventure. Je me souviens également de la pertinence de vos questions lors de mon examen de synthèse et de votre grande capacité d'analyse qui ont sans aucun doute influencé ce travail.

1er et 2e centre, Lyne et Marc. Je ne pouvais vous séparer dans ces remerciements. Vous m'avez accueilli dans la belle Province et surtout vous m'avez vraiment apporté un soutien de tous les instants. J'en suis très reconnaissant.

Ailiers, Rémi à gauche et Guillaume à droite (allez savoir pourquoi ?). Votre compagnie m'a été largement profitable tant lors d'événements festifs que lors de discussions plus poussées pour essayer de refaire le monde…

Arrière, le joueur qui constitue le dernier rempart sur un terrain. Yan, ce poste est à toi, tant pour l'oreille attentive que tu as su me prêter que pour tes judicieux conseils et ta patience.

Dans toute équipe, il y a des **remplaçants** et des **anciens**. Les remplaçants et les anciens font partie intégrante de l'équipe. Je ne vous oublie pas. Merci donc aux

étudiants de maîtrises et aux stagiaires qui se sont succédé au CRP et à Polytechnique lors de mon doctorat et qui ont partagé quelques moments avec moi : Antuan, Axelle, Benoît, Ben, Damien, GDD, Jean-Yves, Marie-Ève, Marie-Hélène, Olivier, Rémi, Romain B., Romain P., Renaud, Seb, Steph, Vincent, Walid, Will. Vous avez largement agrémenté les nombreuses pauses café et autres petits breaks que je me suis autorisés lors de ma période doctorale, que vous soyez présents ou pas d'ailleurs. Vous m'avez permis de relativiser et de me remettre en question sur de nombreux sujets en me rappelant mon âge vénérable, en me taquinant, en me demandant si je pensais finir un jour et autres choses du genre... C'est ça les joueurs remplaçants et les anciens, toujours jaloux des titulaires! Non, sans farce, votre contact a été bénéfique même si je ne l'ai pas forcément montré.

Je ne peux pas oublier non plus le **staff technique**. Merci aux associés de recherche Mao gloglo, Irène, Gabriel, Luciano et Oli. Vous êtes tous intervenus à un moment ou un autre pour me prêter une oreille attentive et pour me faire part de vos judicieux conseils. Sachez que cette aide a été appréciée.

Sponsor : Je remercie Sécurité publique Canada, qui par l'attribution des bourses de recherche en l'honneur de Stuart-Nesbitt White a permis de financer ce travail.

Supporters : la liste est longue et je risquerais d'oublier des noms. Je vais donc remercier ces personnes que je considère comme des amis par groupe. Merci aux gars du Parco. Vous côtoyer sur les vrais terrains de rugby m'a permis de décompresser et de penser à autre chose. Merci aux amis du Québec, de Haute-Savoie, Savoie, Hautes-Alpes, Haute-patate, Nord, Haute-Garonne et autres régions de France et de Navarre. Merci également à Claudette dont la gentillesse et la bonne humeur ont su ensoleiller nombre de mes journées. De manière plus spécifique, je tiens ici à remercier les d'jeunes qui ont contribué à la décoration murale de mon bureau par la création d'œuvres picturales de toute beauté. Gros becs donc à Érine, Marine, Camille, Justine,

Quentin, Ariane et Gabriel. Pourvu que ma prose soit à la hauteur de vos dessins. Merci à l'ensemble de ma famille. Le proverbe « loin des yeux, loin du cœur » ne s'applique véritablement pas pour vous, au contraire. Vous avez su me soutenir dans les bons et les mauvais moments, je vous en remercie. Au moment d'écrire ces lignes, j'ai une pensée particulière pour toi tatan brise-tout.

À tous, du fond de mon cœur, MERCI, quelle belle équipe et quel beau match!!!!

J'espère que vous avez pris autant de plaisir à me côtoyer que j'en ai eu à travailler ou à relaxer avec vous. En tout cas, une équipe de rugby c'est presque une famille et je suis heureux d'avoir pu partager cette expérience doctorale avec vous tous.

Je tiens finalement à remercier les membres de mon jury pour avoir accepté d'évaluer ce travail. De manière plus spécifique, je remercie messieurs Vallerand et Fisher qui ont accepté de juger ce travail bien qu'il soit rédigé dans la langue de Molière et non dans celle de Shakespeare.

RÉSUMÉ

Les infrastructures critiques sont des systèmes complexes. Pour leurs opérations, ces systèmes utilisent de plus en plus des systèmes *Supervisory Control And Data Acquisition* (SCADA). Les méthodes de gestion sont donc de plus en plus dépendantes de l'outil cybernétique, mais également des données nécessaires pour le faire fonctionner. Les infrastructures critiques sont donc vulnérables à la dégradation des données.

Dans ce contexte, mes travaux de recherche visent à développer les bases d'une méthode d'analyse des vulnérabilités des infrastructures critiques face à l'utilisation des données cybernétiques. En caractérisant la vulnérabilité cybernétique des infrastructures critiques, il sera possible d'améliorer la résilience de ces réseaux et de favoriser une approche proactive de la gestion des risques. Il ne s'agit pas de considérer la cybernétique uniquement d'un point de vue attaque de l'infrastructure, mais bien de considérer également l'altération des données.

La première étape consiste à délimiter et à définir le système sur lequel doit se focaliser l'étude de même que la définition du risque utilisée. En considérant le risque comme étant une fonction des aléas, de l'état du système et des conséquences, il est possible de bien délimiter la portée de l'étude. Le système étudié est une infrastructure critique. La vulnérabilité du système est fonction de l'état du système et de la façon dont un aléa peut agir sur cet état et engendrer des conséquences.

La deuxième étape consiste à caractériser une infrastructure critique suivant ses missions, ses fonctions et les ressources qu'elle utilise. Il s'agit de déterminer l'importance des fonctions dans un contexte de continuité opérationnelle. Pour cela, nous nous basons sur des jugements d'experts de manière à différencier les fonctions critiques des fonctions de support. Nous caractérisons également comment la

dégradation de la réalisation d'une fonction peut affecter la réalisation de la mission de l'infrastructure essentielle.

La troisième étape consiste à poser les concepts d'une méthode d'analyse de vulnérabilité. Nous favorisons une approche partant des conséquences (dégradation de la mission) et remontant vers les causes en considérant la variation d'état du système. Pour cela, il est nécessaire de définir la dépendance des fonctions face aux ressources qu'elles utilisent. Il faut donc classer les ressources utilisées suivant leur importance pour la réalisation des fonctions de l'infrastructure critique et caractériser le degré d'affectation de ces fonctions. Pour cela, nous utilisons les principes de l'endorsement.

La dernière étape consiste à regarder plus précisément la dépendance de l'infrastructure critique face à l'utilisation de données cybernétiques. Pour cela, nous considérons les données cybernétiques comme une ressource utilisée particulière. Il s'agit alors de définir les états possibles de ces données. Les critères utilisés sont entre autres les modes de transmission des données de même que le délai existant pour changer d'état.

Les principes et les concepts développés lors de ces travaux de recherche compléteront le travail fait actuellement dans le domaine de la sécurité informatique. En effet, ils considèrent la cybernétique sous un nouvel angle, l'angle de la sûreté de fonctionnement, en se focalisant sur la dépendance des infrastructures critiques face aux données et à leurs transferts.

ABSTRACT

Critical Infrastructures (CIs) are complex systems. For their operations, these infrastructures are increasingly using Supervisory Control And Data Acquisition (SCADA) systems. Management practices are therefore highly dependent on the cyber tools, but also on the data needed to make these tools work. Therefore, CIs are greatly vulnerable to degradation of data.

In this context, this research aims at developing the fundamentals of a method for analyzing the vulnerabilities of CIs towards the use of cyber data. By characterizing cyber vulnerability of CIs, it will be possible to improve the resilience of these networks and to foster a proactive approach to risk management not only by considering cybernetics from a cyber-attack point of view but also by considering the consequences of the use of corrupted data.

The first step of the methodology is to delimitate and define the system that the study should focus on as well as to define the term risk. By considering the risk as a function of hazards, the state of the system and its consequences, it is possible to define the scope of the study. As stated previously, the system studied is a CI. The vulnerability of the system depends on the state of the system itself, on the capacity of a hazard to affect this state and on the undesired consequences the combination of the hazard and the vulnerability will eventually lead to.

The second step is to characterize CIs in terms of their operations, their functions and the resources they use. The idea is to determine the importance of the functions in a context of operational continuity. For this, we rely on expert judgment in order to differentiate the functions that are critical to the good functioning infrastructure and the ones that are supportive. We also characterize how the deterioration of a function can affect the achievement of the mission of the CI.

The third step is to develop the concepts of a methodology for analyzing vulnerability. We here consider an approach based on the consequences (alteration of the mission), and toward the causes considering the variation of the system. For this, it is necessary to define the dependence of each function of the CIs towards the resources they use. We must therefore classify the resources according to their importance for the realization of the functions of the CIs and characterize the level of affectation of these functions whenever a resource is altered or unavailable. For this, we use the principles of endorsement.

The final step consists in looking more specifically the dependence of the CIs towards the use of cyber data. For this, we consider the data as a resource used by the CIs. The objective here is to define the possible states of the data. The criteria used are, among others, the modes of transmission of the data and the time taken to change state.

The principles and concepts developed during this research will complement the works currently done in the field of computer security. Indeed, this research considers cybernetics from a different perspective, the dependence of CIs towards data.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES SIGLES ET ABRÉVIATIONS

ALARP : As low as is reasonably practical.

AMDEC : Analyse des modes de défaillance, de leurs effets et de la criticité.

ANL : Argonne National Laboratory.

BARPI : Bureau d'Analyse des Risques et Pollutions industrielles.

BBC : British Broadcasting Corporation.

BPIEPC : Bureau de la Protection des Infrastructures essentielles et de la Protection civile.

CBRN : Risques chimiques, biologiques, radiologiques et nucléaires.

CCRIC : Centre canadien de réponse aux incidents cybernétiques.

CESG : Communications Electronics Security Group.

CIP/DSS : Critical Infrastructure Protection/Decision Support System.

CIPMA : Critical Infrastructure Protection Modelling and Analysis Program.

CIPTF : Critical Infrastructure Protection Task Force.

CIWIN : Critical Infrastructure Warning Information Network.

CLUSIF : Club de la sécurité des systèmes d'information français.

CNFSH : Comité national français des sciences hydrologiques.

CNVA : Computer network vulnerability assessment program.

CONTEST : United Kingdom Counter Terrorism Strategy.

CPNI : Center for the Protection of National Infrastructure.

CRAIM : Conseil pour la réduction des accidents industriels majeurs.

CRAMM : Central Computer and Telecommunications Agency Risk Analysis and Management Method.

CRP : *Centre risque & performance.*

CRSNG : Conseil de recherches en sciences naturelles et en génies.

CSIRO : Commonwealth Scientific and Industrial Research Organisation.

CSOSG : Programme concepts, systèmes et outils pour la sécurité globale.

DHS : Department of Homeland Security.

EBIOS : Expression of Needs and Identification of Security Objectives.

ÉCR : Évaluation consolidée des risques.

EWS : Early warning system.

FEMA : Federal Emergency Management Agency.

FMECA : Failure mode effects and criticality analysis.

FPM : Faculté Polytechnique de Mons.

GPNC : Groupe de Planification nationale des Contingences.

HAZOP : Hazard and operability study.

HEART : Human error assessment and reduction technique.

I2SM : Infrastructure interdependencies simulation team.

IBM : International Business Machines.

ICE : Infrastructures critiques européennes.

IE : Infrastructure essentielle.

IEN : Infrastructure essentielle nationale.

INCAS : Intégration dans la conception des applications de la sécurité.

INERIS : Institut national de l'environnement industriel et des risques.

INHES : Institut national des hautes études de sécurité.

IRSN : Institut de radioprotection et de sûreté nucléaire.

LANL : Los Alamos National Laboratory.

MADS : Méthodologie d'analyse de dysfonctionnement des systèmes.

MAGDA : Méthode d'administration et de gestion des droits et accréditations.

MARION : Méthodologie d'analyse des risques informatiques orientée par niveaux.

MEEDA : Ministère de l'Écologie, de l'Énergie, du Développement durable et de l'Aménagement du territoire.

MEHARI : Méthode harmonisée d'analyse de risques.

MERMOS : Méthode d'évaluation de la réalisation des missions opérateur pour la sûreté.

MI5 : United-Kingdom's Security Service.

MOSAR : Méthode organisée et systémique d'analyse de risques.

MSP : Ministère de la Sécurité publique du Québec.

NISAC : National Infrastructure Simulation and Analysis Center.

NISCC : National Infrastructure Security Coordination Centre.

NSAC : National Security Advice Centre.

OCDE : Organisation de Coopération et de Développement économique.

OSCQ : Organisation de Sécurité civile du Québec.

OTAN : Organisation du traité de l'Atlantique nord.

PCRII : Programme conjoint de recherche sur les interdépendances des infrastructures.

PEPIC : Programme européen de protection des infrastructures critiques.

PNFIE : Programme national de fiabilité des infrastructures essentielles.

PNSC : Plan national de sécurité civile.

PIC : Protection des infrastructures critiques.

PIE : Protection des infrastructures essentielles.

POE : Plan opérationnel d'entreprise.

POS : Plan opérationnel de sécurité.

PSS : Plan stratégique de sécurité.

PTSP : Programme technique de sécurité publique.

RDDC : Recherche et développement pour la défense Canada.

RNC : Ressources naturelles Canada.

RSSI : Responsable de la sécurité des systèmes d'information.

SCADA : Supervisory Control and Data Acquisition.

SHERPA : Systematic human error reduction and prediction approach.

SNL : Sandia National Laboratories.

SNPIE : Stratégie nationale de protection des infrastructures essentielles.

SPC : Sécurité publique Canada.

TESEO : Tecnica empirica stima errori operatori.

THERP : Technique for human error rate prediction.

TISN : Trusted Information Sharing Network.

UIT : Union Internationale des Télécommunications.

LISTE DES ANNEXES

INTRODUCTION

Les infrastructures essentielles, aussi appelées infrastructures critiques ou infrastructures vitales, sont des éléments prépondérants pour le fonctionnement de la société civile. En effet, les infrastructures essentielles font partie des structures organisationnelles qui ont pour mandat de fournir les ressources et les services qui soutiennent le déroulement des activités socio-économiques des sociétés actuelles. De ce fait, il apparaît nécessaire de les maintenir fonctionnelles autant sur une base d'opérations quotidiennes qu'en situation d'urgence.

Ces entités qui étaient historiquement séparées physiquement sont, du fait des progrès de la technologie, de plus en plus interconnectées formant ainsi des réseaux d'infrastructures. Elles sont constituées d'un ensemble de composantes qui forment à leur tour des réseaux principaux et secondaires. L'ensemble forme un système intégré dont la fiabilité est dépendante de la performance de l'ensemble des composantes des différentes infrastructures essentielles. C'est dans cette forme d'organisation systémique que réside la force, mais également la vulnérabilité des infrastructures essentielles.

En effet, l'organisation des infrastructures essentielles en réseaux les renforce, car il est ainsi possible de mettre en œuvre des éléments de redondance. Cependant, cela constitue également une faiblesse dans le sens où la défaillance d'une infrastructure essentielle peut entraîner les défaillances en cascade des autres infrastructures essentielles dépendantes.

Il est donc important de renforcer ces réseaux de manière à permettre de diminuer les vulnérabilités de la société civile qui est dépendante des ressources fournies par les différentes infrastructures essentielles.

Actuellement, les processus d'analyse et de gestion des risques spécialement dédiés aux infrastructures essentielles et à leurs interdépendances commencent à se développer. Ces développements se font principalement en réaction aux attentats

terroristes qui sont survenus depuis le début du XXIe siècle, mais aussi en raison des forts changements se produisant au niveau environnemental. Il devient donc très important de renforcer la société face à ces nouveaux types de menace de façon à pouvoir favoriser un développement durable. En effet, analyser et gérer les risques reliés aux infrastructures essentielles devient primordial dans le sens où elles sont développées pour répondre tant aux besoins actuels qu'à ceux des générations futures.

De manière classique, les méthodes d'analyse de risques se focalisent principalement sur la prise en compte des aléas pouvant affecter une infrastructure essentielle et sur la considération des conséquences pouvant être engendrées par sa défaillance.

Toutefois, dans le domaine de la gestion des risques, une nouvelle tendance vise à aborder une autre composante du risque en considérant la vulnérabilité des systèmes analysés de manière à améliorer leur résilience. Il est cependant parfois difficile de véritablement différencier les notions se cachant derrière l'utilisation des termes de risque, vulnérabilité ou résilience.

Une autre problématique est importante à intégrer dans la gestion des risques associés aux infrastructures essentielles. Il s'agit de la prise en compte des vulnérabilités reliées à l'utilisation de l'outil informatique.

Depuis le milieu du XXe siècle, l'informatique et les technologies qui s'y rattachent n'ont cessé de se développer apportant des transformations majeures dans les modes de gestion des différents secteurs d'activité des sociétés industrialisées. Le fort développement des systèmes informatiques associés à des moyens de communication de plus en plus puissants, tels qu'Internet, a donné naissance à ce qu'il est possible de qualifier d'ère de l'information (Castells, 2001). Ces changements profonds modifient grandement les modes de communication et de gestion des sociétés industrialisées.

L'opération et la gestion des infrastructures essentielles ne font pas exception dans ce contexte d'utilisation et de dépendance croissante face à l'utilisation des systèmes informatisés et des systèmes de contrôle tels que les systèmes SCADA.

Les infrastructures essentielles sont renforcées par une augmentation des informations disponibles qui leur permettent de gérer de manière plus efficace et plus rapide les changements pouvant survenir tant à leur niveau qu'au niveau de l'environnement qui les entoure. Cependant, elles peuvent également être affaiblies par un afflux trop grand de données mises à leur disposition. En effet, trop d'information tue l'information. Il peut devenir difficile de retrouver la bonne information au bon moment de manière à pouvoir faire face efficacement à une situation donnée.

En perdant leur indépendance, les infrastructures essentielles sont de plus en plus vulnérables aux effets domino. L'informatisation croissante de ces réseaux augmente cette vulnérabilité en facilitant les transferts de vulnérabilités entre infrastructures essentielles (Ministère Fédéral de l'Emploi et du Travail, 2000 ; Robert et coll., 2002).

Une bonne connaissance de la dynamique de ces transferts est essentielle de façon à éviter que des dysfonctionnements bénins ne se transforment en situation de crises majeures.

La crise du verglas de 1998 au Québec et en Ontario et les craintes quant au « bogue de l'an 2000 » sont de parfaits exemples de la vulnérabilité d'une infrastructure essentielle aux effets domino. La tempête de verglas qui a eu lieu du 5 au 9 janvier 1998 a mis à rude épreuve le réseau de télécommunications tant directement que par l'intermédiaire de la défaillance du réseau de distribution d'électricité comme le souligne le rapport Nicolet (Nicolet et Coll., 1999). Cet événement exceptionnel démontre bien la vulnérabilité de l'ensemble des infrastructures essentielles qui utilise de plus en plus des systèmes d'automatisation

et de contrôle à distance. Cependant, l'aléa naturel n'est pas le seul à pouvoir affecter les infrastructures. Elles sont particulièrement vulnérables aux aléas techniques et humains. Les pannes électriques survenues en Amérique du Nord et en Italie durant l'été et l'automne 2003 sont de parfaites illustrations d'une combinaison de défaillances externes, techniques et humaines, qui vont engendrer le dysfonctionnement des systèmes informatiques d'autres réseaux. D'un autre côté, comme le souligne Langlois (1995), la plus grande menace pesant sur les systèmes informatiques est interne. Elle est à la fois liée aux erreurs, commises par mégarde ou inexpérience, et aux actes de malveillance pouvant être posés par les salariés des entreprises ainsi qu'à l'utilisation combinée de matériels de diverses générations, les plus anciens et les moins perfectionnés pouvant fragiliser le système. Les systèmes informatiques qui sont à la base du fonctionnement des infrastructures essentielles sont donc vulnérables à de nombreux aléas tant internes qu'externes.

De manière classique, la prise en compte de l'outil informatique dans le domaine des risques se fait sous l'angle de la sécurité et sert à tenter de se prémunir face à des actes de malveillance. Ce mode de prise en considération de l'informatique dans le domaine des risques ne semble pas suffisant pour se prémunir face à des défaillances en cascade.

Il paraît également important de prendre en compte l'informatique en s'interrogeant sur la dépendance des infrastructures essentielles face à l'obtention et à l'utilisation des données qui sont nécessaires à leur fonctionnement.

Il s'agit de considérer les données du point de vue du risque informatique, et donc de la sécurité face à des actes de malveillance, mais aussi d'intégrer les notions de qualité des données. Il faut à la fois s'intéresser à la donnée et à son mode de transfert et donc aborder cette problématique sous l'angle de la cybernétique. Il faut, en effet, pouvoir considérer la dépendance des infrastructures essentielles face à l'utilisation des données mais également pouvoir caractériser la capacité d'adaptation du système en relation avec la dégradation éventuelle de ces données.

Pour gérer les vulnérabilités des infrastructures essentielles, il est primordial de comprendre comment elles sont organisées, mais également comment la dégradation des données est intégrée dans les principes de gestion. Les modes de défaillances peuvent être multiples en liaison avec les propriétés-mêmes des systèmes informatisés (technologie, code pouvant être plus ou moins adapté ou validé, connaissances nécessaires à son utilisation, etc.), mais également en raison des différents aléas pouvant les affecter (connaissances mal adaptées, mauvaises utilisations, mauvaises données, actes de malveillance pouvant affecter à la fois la technologie, le code ou les connaissances, etc.).

Dans ce contexte, ce travail vise dans un premier temps à proposer une définition globale du risque et des termes qui lui sont reliés de manière à, dans un deuxième temps, poser les bases d'une méthodologie d'analyse des vulnérabilités adaptée aux infrastructures essentielles en se concentrant plus particulièrement sur la problématique de leurs dépendances face à la cybernétique.

CHAPITRE 1 REVUE DE LITTÉRATURE

Ce travail porte sur la prise en compte du risque cybernétique dans le mode de fonctionnement des infrastructures essentielles. Il vise donc à considérer l'outil informatique et l'utilisation des données dans la gestion opérationnelle et le contrôle d'une infrastructure essentielle.

L'objectif final est de définir les vulnérabilités des infrastructures essentielles, engendrées par les données cybernétiques, au niveau de leurs opérations.

Le but de ce travail, même s'il paraît simple dans sa formulation, à tout le moins tel qu'elle est présentée dans l'introduction, n'en demeure pas moins complexe du fait qu'il touche un domaine relativement nouveau, la protection des infrastructures essentielles et, car il fait appel à de nombreuses notions.

Cette revue de littérature, nous permettra de définir ce que sont les infrastructures essentielles et comment sont analysées leurs interdépendances. Elle permet également de revenir sur la problématique de l'analyse des risques reliée au domaine des contrôles à distance et de l'informatique.

1.1 Les infrastructures essentielles

La majorité des écrits traitant des « mégastructures » parle d'infrastructures essentielles ou d'infrastructures critiques qui sont des traductions littérales du terme anglais *critical infrastructures*. Le terme d'infrastructures essentielles est normalisé au Canada par Sécurité publique Canada (SPC) qui les définit comme *« les installations, réseaux, moyens et biens physiques et ceux de la technologie de l'information, dont la défaillance ou la destruction entraînerait de graves répercussions sur la santé, la sécurité ou le bien-être économique des Canadiens et des Canadiennes, ou encore sur le bon fonctionnement des gouvernements du pays »* (SPC, 2008a). Au Canada, les infrastructures essentielles comprennent dix secteurs interdépendants (Tableau 1.1).

Tableau 1.1 - Les secteurs des infrastructures essentielles (SPC, 2008a).

Secteur	Sous-secteurs
Énergies et services publics	Systèmes de production d'énergie électrique, de gaz naturel et de pétrole, ainsi que leurs réseaux de transport
Technologies de l'information et des communications	Systèmes, logiciel, matériel et réseaux de télécommunications et de radiodiffusion, y compris Internet
Finance	Opérations bancaires, valeurs mobilières et investissements
Soins de santé	Hôpitaux, établissements de soins de santé et de réserve de sang, laboratoires et produits pharmaceutiques
Nourriture	Sécurité, distribution, agriculture et industrie alimentaire
Eau	Eau potable et gestion des eaux usées
Transports	Voies aériennes, ferroviaires, maritimes et terrestres
Sécurité	Sécurité contre les armes chimiques, biologiques, radiologiques et nucléaires, matières dangereuses, recherche et sauvetage, secours d'urgence et barrages
Gouvernement	Services, installations, réseaux d'information, biens gouvernementaux et sites et monuments nationaux privilégiés
Fabrication	Base industrielle de la défense, industrie chimique

Le terme d'infrastructure essentielle, tel qu'il est défini, regroupe donc de nombreux secteurs de natures différentes. De manière plus spécifique, cette thèse porte sur une des composantes des infrastructures essentielles que sont les réseaux « industriels » qui offrent des biens et des services. Il est possible de nommer, entre autres, les secteurs de l'énergie, des technologies de l'information et des communications, de l'eau et des transports.

Les infrastructures essentielles constituent donc des rouages primordiaux pour l'activité socio-économique du Canada. En cela, il s'avère donc nécessaire de leur apporter une attention particulière en les protégeant au mieux et en adoptant une meilleure gestion des risques, tels que le précise Sécurité publique Canada (SPC, 2008a).

Les travaux visant à protéger les infrastructures essentielles se sont véritablement développés depuis 1996 avec la mise en place aux États-Unis de la *President's Commission on Critical Infrastructure Protection* (Clinton, 1996). Depuis lors, la problématique de la sûreté et de la sécurité des infrastructures essentielles s'intensifie et de plus en plus de groupes de recherche tentent d'y apporter des réponses pratiques.

Les travaux qui se font sur les infrastructures essentielles sont de deux ordres :

- sectoriels ;
- intersectoriels.

1.1.1 Travaux sectoriels

Les travaux sectoriels visent, comme leur nom l'indique, à étudier les risques dans un secteur particulier, tels que l'énergie (réseaux électriques, nucléaires, etc.), les transports (aéronautique, aérospatial, etc.) et la fabrication (industrie chimique, alimentaire, etc.). Le développement des techniques d'analyse des risques dans ces secteurs précis s'explique par le besoin de renforcer les niveaux de sécurité face à des événements extrêmes. Dans ces domaines précis, de nombreuses méthodes

d'analyse de risques ont été développées en réaction à des défaillances importantes, telles que la panne électrique de 2003 en Amérique du Nord (Ressources naturelles Canada [RNC], 2008), l'accident chimique de Seveso en Italie en 1976 (Bureau d'Analyse des Risques et Pollutions industrielles [BARPI], 2008), les accidents nucléaires de Three Mile Islande en 1979 aux États-Unis (Dickinson College, 2008) et de Tchernobyl en 1986 (Institut de radioprotection et de sûreté nucléaire [IRSN], 2008) en Ukraine ainsi que les attentats du 11 septembre 2001 aux États-Unis (Federal Emergency Management Agency [FEMA], 2002).

Parmi l'ensemble des travaux existants, les recherches menées par la Faculté Polytechnique de Mons (FPM) en Belgique sont intéressantes dans le sens où elles essaient de caractériser les enchaînements de défaillances menant à une réaction en chaîne.

Ces travaux font suite à la directive Seveso du 9 décembre 1996 et plus particulièrement à l'article 8 de cette directive (Ministère fédéral de l'Emploi et du Travail, 2000). Cette directive du 24 juin 1982 avait pour but de doter les États européens d'une politique commune en matière de prévention des risques industriels majeurs. À partir du 3 février 1999, la directive Seveso a été remplacée par la directive Seveso II (directive 96/82/CE) qui impose aux exploitants d'industries classées à risque de mettre en œuvre un système de gestion de la sécurité et de maîtrise du danger comprenant notamment la mise en œuvre de processus d'information et de participation du public (Ministère de l'Écologie, de l'Énergie, du Développement durable et de l'Aménagement du territoire [MEEDA], 2008a).

Dans le cadre de ces travaux, la FPM a défini un effet domino comme une cascade d'accidents dans laquelle les conséquences des accidents précédents sont accrues par les accidents suivants, conduisant à un ou des accidents majeurs.

Par la suite, la FPM a adapté cette définition à son champ d'application à savoir l'industrie chimique. Pour ce faire, elle définit comme primaire un premier accident qui va alors concerner un équipement primaire. Pour considérer les effets domino, elle définit que les effets primaires induisent la défaillance d'un second équipement alors qualifié de secondaire qui est à son tour le siège d'un accident qualifié de secondaire (Faculté Polytechnique de Mons, 1998).

La méthode développée a pour but d'essayer de définir les enchaînements d'événements exceptionnels de type explosion ou incendie entre des industries utilisant des produits chimiques. Elle ne permet donc pas de considérer l'ensemble des vulnérabilités d'une infrastructure essentielle.

Aux États-Unis, les travaux de Mili, Qiu et Phadke (2004) abordent également cette problématique des défaillances en cascades d'infrastructures essentielles. Cette fois-ci, ce sont les systèmes électriques qui sont considérés. La méthodologie consiste à développer des algorithmes de calculs permettant d'évaluer les risques associés aux réseaux électriques en considérant notamment les points faibles des systèmes de protection. Pour cela, les auteurs ont développé une approche statistique basée sur des données historiques. L'objectif ultime est de développer une méthodologie d'évaluation des risques adaptée aux réseaux électriques à grande échelle.

De nombreux autres travaux abordant la problématique de la défaillance et des effets domino entre infrastructures essentielles de même nature existent. Nous ne les présenterons pas. Il est intéressant de savoir que de nombreux secteurs d'infrastructures essentielles abordent la problématique des défaillances et des interdépendances intrasectorielles.

Cependant, il semble plus intéressant dans un contexte de continuité opérationnelle et de mesures d'urgence de regarder les travaux qui considèrent plus spécifiquement le problème des interdépendances et des répercussions (effet boule

de neige et effet domino) de la défaillance d'une infrastructure essentielle sur les activités d'une infrastructure essentielle de nature différente. Ces travaux qui sont relativement plus récents que ceux se focalisant sur un type donné d'infrastructure essentielle peuvent être qualifiés d'intersectoriels.

1.1.2 Travaux intersectoriels

Ces travaux se focalisent sur la caractérisation des dépendances et des interdépendances existant entre différentes infrastructures essentielles. Pour cela, ils déterminent et analysent les liens et les transferts de vulnérabilités existants entre les infrastructures essentielles (Figure 1.1).

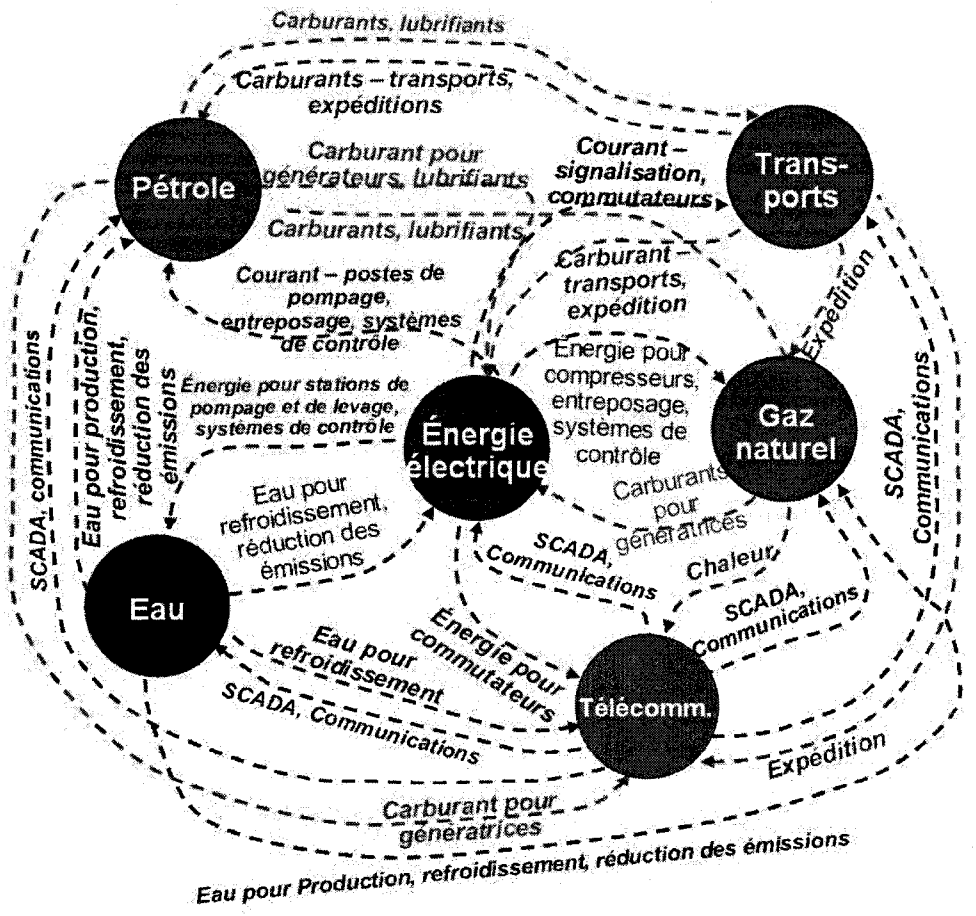

Figure 1.1 - Exemple d'interdépendances entre infrastructures essentielles (traduit de Rinaldi et coll., 2001).

De par le monde, les programmes de recherche portant sur l'analyse des interdépendances entre infrastructures essentielles ne se développent véritablement que depuis les années 2000. De plus en plus de modèles de simulation tendent à se développer (Pederson et coll., 2006).

D'après les résultats publiés, trois régions se démarquent plus particulièrement dans ce domaine de recherche à savoir, l'Australie, l'Amérique du Nord (États-Unis et Canada) et l'Europe. En Australie, le *Critical Infrastructure Protection Modelling and Analysis Program* (CIPMA) du gouvernement vise à assurer la protection des infrastructures essentielles et à améliorer la résilience de la société et de l'économie du pays. Aux États-Unis, le *National Infrastructure Simulation and Analysis Center* (NISAC) et l'*Argonne National Laboratory* (ANL) effectuent des recherches sur les infrastructures critiques et leurs interdépendances. En Europe, les approches de la Grande-Bretagne et de la France privilégient la protection des infrastructures essentielles face aux risques terroristes. Les Pays-Bas, quant à eux, favorisent une approche plus globale. Au Canada, en 2000, le Groupe de Planification nationale des Contingences (GPNC) a initié des recherches en ce qui a trait aux interdépendances entre les infrastructures critiques. Plus récemment, le Programme conjoint de recherche sur les interdépendances des infrastructures (PCRII) de Sécurité publique Canada et du Conseil de recherches en sciences naturelles et en génies (CRSNG) a eu comme objectif de faire avancer les connaissances dans le domaine de la gestion des risques appliquée aux infrastructures essentielles afin d'assurer leur sécurité et les protéger. Des résumés de ces travaux de recherche sont présentés ci-après.

1.1.2.1 Travaux en Australie

Les travaux australiens sont particulièrement intéressants. En effet, les législations australienne et néo-zélandaise, et plus particulièrement la norme de gestion des risques (AS/NZS 4360), servent de base au Ministère de la Sécurité publique du Québec (MSP) pour élaborer son cadre de référence pour la gestion des risques (MSP, 2007a). De plus, ces travaux, faisant l'objet d'échange avec les

gouvernements états-uniens et britanniques (Scott, 2007), sont également intéressants, car les programmes australiens à l'instar des États-Uniens font figure de pionniers dans le domaine de l'analyse et de la gestion des risques pour les infrastructures essentielles (Cobb, 1997; Cobb, 1999).

Le principal programme australien portant sur les infrastructures essentielles est le CIPMA qui est un projet gouvernemental initié par le département de la justice (Attorney-General), en partenariat avec *Geoscience Australia* et le *Commonwealth Scientific and Industrial Research Organisation* (CSIRO). Ce programme a pour but d'analyser et de modéliser les défaillances en cascade d'infrastructures essentielles.

L'approche mise en œuvre nécessite la participation de nombreux partenaires industriels dans le sens où ce sont eux qui possèdent et gèrent environ 90% des infrastructures essentielles (Scott, 2007). Cette approche est une approche inductive se concentrant sur l'analyse géomatique à grande échelle de scénarios de danger (CSIRO, 2008). À partir d'un aléa naturel ou humain, les outils informatiques développés permettent de modéliser les défaillances en cascade anticipées en intégrant la prise en compte des vulnérabilités des infrastructures essentielles. Pour cela, ces travaux se basent sur la mise en œuvre d'un réseau de travail, le *Trusted Information Sharing Network* (TISN), de façon à favoriser un climat de confiance entre les partenaires du projet de manière à permettre l'échange de données pouvant être sensibles du point de vue de la sécurité. L'objectif visé étant de définir :

- le comportement des infrastructures essentielles ;
- le degré d'affectation de la population et de l'économie ;
- la durée de cette affectation ;
- le secteur affecté.

Cette approche et ses objectifs semblent intéressants de par leur considération des effets domino, mais également par la considération du triptyque aléas/vulnérabilités/conséquences pour définir le risque.

Ces travaux se trouvent cependant limités, car ils n'intègrent que peu de secteurs d'activité différents. Ils se concentrent sur l'énergie, les finances et les télécommunications.

De plus, la problématique du risque cybernétique associé à l'opération des réseaux n'est pour le moment pas abordée dans le programme CIPMA (Scott, 2007).

Un autre programme australien, le *Computer network vulnerability assessment program* (CNVA), piloté par le *Australian Government Computer Emergency Readiness Team* (GovCERT.au) est spécifiquement dédié à l'étude des vulnérabilités et des défaillances reliées aux infrastructures essentielles du secteur des technologies de l'information et des télécommunications (TISN, 2008).

Ce programme vise plus à considérer les vulnérabilités de ces infrastructures essentielles particulières et les défaillances qu'elles pourraient engendrer. De plus, il aborde la problématique des vulnérabilités cybernétiques sous l'angle de la sécurité informatique (virus, vers, etc.).

La qualité de service des infrastructures essentielles fournissant ou servant aux transferts des données ne semble pas véritablement prise en compte. Un autre élément important ne semblant pas être considéré est la dépendance des infrastructures essentielles face à l'utilisation des données.

Les deux programmes développés en Australie présentent un autre inconvénient dans le sens ou l'utilisation de système d'information géographique, bien que représentant un outil très puissant, est très demandant au niveau financier, mais également en ce qui a trait à toute l'information nécessaire pour faire fonctionner les modèles (Robert et Cloutier, 2007).

Cette approche est donc possible si elle est soutenue par un gouvernement et par une forte volonté politique. La mise en œuvre d'un tel programme semble

cependant plus difficile au Québec où la responsabilité de la sécurité civile incombe d'abord et avant tout aux autorités locales et régionales (Éditeur officiel du Québec, 2008).

1.1.2.2 Travaux aux États-Unis

Les premiers travaux concernant les interdépendances entre infrastructures essentielles aux États-Unis sont ceux du NISAC qui est né du partenariat entre le *Los Alamos National Laboratory* (LANL) et le *Sandia National Laboratories* (SNL) sous l'égide du *Department of Homeland Security's Preparedness Directorate*. En effet, le 26 octobre 2001, le Congrès américain désigne le NISAC comme source de compétence en ce qui a trait à la protection des infrastructures critiques et au support pour les activités visant à contrer le terrorisme, à évaluer les menaces et à atténuer les risques.

La mission du NISAC est de fournir des modèles et des simulations adaptés à l'analyse des infrastructures critiques, de leurs interdépendances et de leurs vulnérabilités. Le but étant de rendre plus résistantes les infrastructures essentielles nationales (IEN) en servant de soutien aux décideurs. Ce soutien s'effectue plus particulièrement dans les domaines de l'évaluation de politiques, de programmes d'investissements et d'atténuation de même que dans les domaines de la formation et de l'intervention d'urgence (NISAC, 2003).

Le NISAC a mis en place divers programmes de formation et de recherche. Parmi ceux-ci deux aspects se révèlent plus particulièrement intéressants :

- la modélisation des interdépendances;
- l'analyse des conséquences.

La modélisation des interdépendances des réseaux se fait essentiellement en se basant sur l'expertise développée par le SNL en ce qui a trait à la simulation des systèmes complexes. Le NISAC cherche tout d'abord à cartographier les « nœuds critiques » dans les systèmes des infrastructures. Ensuite, il quantifie les

conséquences physiques et économiques d'un danger pour la sécurité du système des infrastructures essentielles nationales.

Actuellement, le NISAC développe une méthode de simulation informatisée qui tente de prédire, en temps réel, les conséquences d'événements perturbateurs sur les infrastructures critiques.

L'approche du NISAC nécessite des ressources importantes, telle que l'utilisation d'ordinateurs très puissants pouvant supporter les simulations de divers systèmes complexes. Ceci peut rendre difficile l'application de cette méthodologie par des infrastructures essentielles ou des groupes ne disposant pas de moyens aussi importants que ceux du NISAC.

D'autre part, cette méthodologie est basée sur une approche par scénario qui rend plus difficile la prise en considération de l'ensemble des événements pouvant conduire à la défaillance d'un système par l'intermédiaire d'effets domino. Elle est adaptée à l'étude des transferts d'aléas se propageant par l'intermédiaire de liens permanents (physiques) entre réseaux.

Des études centrées sur les conséquences sont également développées au NISAC en complément de leur approche de simulation des interdépendances entre infrastructures critiques. Ces études ont pour but d'augmenter l'évaluation des risques reliés aux infrastructures essentielles nationales.

Des techniques déductives (diagrammes en blocs, arbres de défaillance, diagrammes d'influence) sont utilisées pour décomposer de façon systématique chaque conséquence indésirable en une série de conditions immédiates, nécessaires et suffisantes pouvant la générer. Ces causes techniques, humaines et naturelles peuvent par la suite être associées aux propriétés particulières d'une infrastructure donnée.

Cette méthodologie présente l'avantage de vouloir brosser un portrait complet des aléas pouvant mener à la défaillance d'une infrastructure et par la même à des conséquences. Cependant, tout comme la méthodologie précédente, l'approche basée sur les conséquences utilise des scénarios ce qui peut mener à sous-estimer les enchaînements d'aléas pouvant conduire à la défaillance d'un système. De plus, cette approche basée sur le coût des défaillances, même si elle s'avère très utile pour le renforcement des infrastructures, peut se révéler discutable en cas de sinistre. En effet, au moment de l'analyse a posteriori d'un événement catastrophique, il peut être difficile de justifier les décisions prises uniquement sur la base d'une approche coûts-bénéfices.

Ces dernières années, les travaux du NISAC se focalisent de plus en plus sur l'analyse de secteurs spécifiques, tels que les réseaux de l'énergie (Ellison, 2007), des télécommunications (Conrad and O'Reilly, 2006) et de la finance (Beyeler et coll., 2006 ; Soramäki et coll., 2007), en les considérant comme étant au cœur des réseaux (interdépendances) (Conrad et coll., 2006).

Ces travaux se caractérisent principalement par une évaluation économique des risques. Les travaux portant sur les technologies de l'information et les réseaux de télécommunications abordent les risques en considérant les liens cybernétiques, mais pas forcément la dépendance des infrastructures essentielles face à la dégradation des données cybernétiques. En ce sens, ils sont plus recentrés sur la qualité de fonctionnement de l'infrastructure essentielle que sur sa qualité de service. Cependant, ces deux notions de qualité (fonctionnement et service) sont indispensables pour la réalisation des missions des réseaux de télécommunications ou des technologies de l'information comme le précise l'Union internationale des télécommunications (UIT) (UIT-T, 2005). Il apparaît donc primordial de considérer la qualité de service des réseaux de télécommunications en prenant en compte la dépendance des infrastructures essentielles face à l'utilisation de données cybernétiques.

De manière plus spécifique, en ce qui a trait au risque cybernétique, les travaux du NISAC se focalisent principalement sur les attaques cybernétiques de façon à améliorer la protection des réseaux face à ces menaces (SNL, 2008). À l'instar des travaux australiens, les travaux du NISAC ne semblent pas intégrer la vulnérabilité des infrastructures essentielles face à la cybernétique prise dans le sens de la communication et de la dépendance aux informations.

Certains des travaux de recherche du NISAC, en particulier le développement du *Critical Infrastructure Protection/Decision Support System* (CIP/DSS), se font en partenariat avec d'autres groupes de recherche, en particulier l'ANL. Le CIP/DSS est intéressant, car il vise à supporter la prise de décision des gestionnaires pour la protection des infrastructures essentielles (Conrad et coll., 2006). Pour cela, il simule les interdépendances directes entre infrastructures essentielles en se basant sur les ressources clés utilisées ou produites par ces infrastructures, mais aussi sur les conséquences environnementales, économiques et au niveau de la santé humaine. Ce concept de ressources clés est très intéressant, car il permet d'étudier le système en se focalisant sur ses besoins, mais également sur ses apports à la société (Conrad et coll., 2006).

Parmi les travaux portant sur les interdépendances entre infrastructures essentielles, les travaux de l'ANL se démarquent de par la forte expertise développée dans ce domaine.

Les travaux de l'ANL sont développés sous l'égide d'un de ses centres de recherche, l'*Infrastructure Assurance Center* (IAC) qui a pour objectif de fournir des services et de supporter les organisations tant publiques que privées intervenant dans les domaines des mesures d'urgence (prévention, préparation, intervention et rétablissement) associées aux infrastructures essentielles (ANL, 2008).

Les recherches de ce centre se focalisent sur la sécurité et la fiabilité des infrastructures critiques américaines, plus particulièrement le secteur énergétique,

et des ressources qu'elles fournissent qui sont essentielles pour l'économie et le gouvernement américain.

Pour cela, le centre privilégie une approche tous risques intégrant à la fois les aléas naturels, techniques et sociaux et considérant les conséquences sur la santé humaine, l'économie et la sécurité nationale. Il base également ses analyses sur le type de lien caractérisant les interdépendances.
Quatre types de lien ont été définis :

- physique (lien direct d'utilisation par une infrastructure d'une ressource fournie par une autre infrastructure) ;
- cybernétique (électronique, informationnel, systèmes SCADA) ;
- géographique (corridor commun) ;
- logique (dépendance par l'entremise des marchés financiers).

L'approche développée par l'ANL est également intéressante de par sa définition du concept de risque intégrant à la fois les aléas, les vulnérabilités et les conséquences pouvant affecter les liens entre infrastructures essentielles. La vulnérabilité est abordée sous l'angle de la sensibilité du fonctionnement des infrastructures essentielles en regard des différents liens qui les relient. L'analyse de risque se concentre donc principalement sur les interdépendances et donc sur les liens existants entre les infrastructures essentielles.

L'approche de l'ANL se démarque également, car elle ne se limite pas aux liens entre infrastructures essentielles. En effet, ces travaux considèrent également le mode de fonctionnement des infrastructures essentielles.

Chaque fonction constituant le système peut être analysée suivant ses équipements, mais aussi en considérant les ressources qu'elle utilise ou fournit. De plus, à l'intérieur même du système, il existe des interdépendances qu'il faut considérer.

Du point de vue de la vulnérabilité cybernétique, les travaux de l'ANL se focalisent sur la caractérisation des interdépendances relatives au lien cybernétique. Ils analysent les dépendances reliées à la collecte de données, au contrôle et à la gestion des infrastructures essentielles. La cybernétique est donc prise en compte sous l'angle de l'informatique, l'électronique et les liens informationnels. La vulnérabilité des infrastructures essentielles est considérée face à la dégradation du lien cybernétique.

L'ANL a développé de nombreux outils informatiques pour identifier les interdépendances et pour partager les informations pertinentes entre les organisations parties prenantes du projet (Peerenboom and Fisher, 2007).

Pour cela, ils tentent de répondre aux questions suivantes :

- connaissez-vous vos fournisseurs et leurs chaînes d'approvisionnement ?
- connaissez-vous les effets domino qui pourraient résulter d'une défaillance ?
- connaissez-vous les systèmes de relève qui sont en place ?
- connaissez-vous l'autonomie de ces systèmes de relève ?
- savez-vous où trouver de l'information concernant les priorités de rétablissement des infrastructures ?

Afin de partager adéquatement ces informations, le *Department of Homeland Security* (DHS) a mis en place un programme d'échange d'information entre le secteur privé et le gouvernement, le *Protection Critical Infrastructure Information* (DHS, 2008). Ce programme est basé sur le volontariat. Les gestionnaires d'infrastructures essentielles peuvent y participer en partageant leurs données.

Les informations et données résultant des questions précédemment présentées permettent de faire fonctionner différents outils informatiques développés par l'ANL. La majorité de ces outils sont des systèmes d'information géographique servant à la représentation cartographique de l'état des infrastructures essentielles à l'échelle du pays. Ils servent également à l'analyse géospatiale des informations

concernant les infrastructures essentielles. Pour cela, ils utilisent GeoPDF qui permet à partir d'Adobe Reader de partager et de gérer des cartographies. L'avantage de GeoPDF est qu'il est facilement accessible et est relativement convivial dans son utilisation. Il apporte également les avantages des logiciels de la gamme Adobe en ce qui concerne la capacité de protection des données.

Des outils de visualisation en 3D des infrastructures essentielles, telles qu'ANL Viz Tool, sont également développés ce qui permet de mieux comprendre les interdépendances et les zones de faiblesse caractérisant les liens physiques entre différentes infrastructures essentielles.

Le dernier type d'outil développé est un outil d'analyse des services de rétablissement des infrastructures essentielles, Restore©, utilisant des probabilités pour caractériser la variabilité des délais de mise en œuvre des différentes étapes nécessaires au rétablissement.

1.1.2.3 Travaux en Europe

Il est également intéressant de regarder ce qui se fait au niveau de l'Europe puisqu'elle constitue une entité économique importante. Plusieurs états constitutifs de l'Union européenne ont initié des travaux en ce qui a trait à la protection des infrastructures critiques. Ces préoccupations de protection ont débuté à la fin du XXe siècle relativement aux tensions existant en raison de la guerre froide. À la chute du bloc de l'est, ces préoccupations se sont estompées pour refaire surface à l'aube de l'an 2000 en raison des problèmes informatiques anticipés pour le passage au nouveau millénaire. Ce besoin d'analyser et de protéger les infrastructures essentielles s'est amplifié ces dernières années relativement à la peur du terrorisme découlant des attentats du 11 septembre 2001 aux États-Unis et plus récemment de ceux de mars 2004 en Espagne et de juillet 2005 en Grande-Bretagne.

1.1.2.3.1 Travaux en Grande-Bretagne

En Grande-Bretagne, les travaux dans le domaine de la protection des infrastructures essentielles sont principalement axés sur le risque terroriste. Cet état de fait s'explique par l'histoire de la Grande-Bretagne et en particulier par les problématiques reliées à l'Irlande du Nord et aux actions de l'armée républicaine irlandaise. Les attentats de Londres des 7 et 21 juillet 2005 ont renforcé ce besoin de diminuer les vulnérabilités de la société britannique face aux nouvelles menaces terroristes. Ces menaces sont prises très au sérieux, car, en plus d'être spectaculaires, elles engendrent des conséquences très importantes. Le 7 juillet 2005 à Londres, quatre explosions ont touché les transports publics de la ville, faisant 52 morts et plus de 770 blessés (BBC News, 2008). Le 21 juillet 2005, quatre autres attentats à la bombe ont de nouveau été perpétrés contre les transports en commun de la capitale britannique ne faisant heureusement que des dégâts matériels (BBC News, 2008).

Ces attentats ont démontré la vulnérabilité des infrastructures essentielles britanniques tant au niveau des transports qu'au niveau des télécommunications (circulation de l'information) et des organismes gouvernementaux. Ils ont montré la nécessité d'améliorer le niveau de protection des infrastructures essentielles sur le territoire britannique. Pour cela, un programme de contre terrorisme a été mis en place pour différents secteurs :

- les représentations diplomatiques ;
- les sites symboliques et touristiques ;
- les transports ;
- les institutions financières ;
- les sites stratégiques.

Pour répondre à ces événements simultanés maximisant les conséquences, le *Home Office* et *New Scotland Yard* ont mis en œuvre un programme stratégique (*United Kingdom Counter Terrorism Strategy* : CONTEST) visant à réduire le risque

(Home office, 2008 ; Clancy, 2008). Ce programme comprend quatre missions autour de deux axes principaux :

- la réduction de la menace : prévenir le terrorisme en se basant sur ses causes, poursuivre les terroristes et ceux qui les supportent ;
- la réduction de la vulnérabilité des infrastructures essentielles : protéger le public et les intérêts britanniques, se préparer aux conséquences en augmentant la résilience face à la menace terroriste.

Les objectifs du programme CONTEST sont les suivants :

- sauver des vies ;
- protéger l'économie ;
- protéger les infrastructures essentielles ;
- construire une société résiliente ;
- favoriser la continuité opérationnelle ;
- augmenter les capacités.

Pour ce faire, le programme CONTEST se base sur la vidéosurveillance et sur le partage d'informations entre les organismes gouvernementaux. Ce programme a permis de comprendre le mode d'action des terroristes lors des événements de juillet 2005. Cependant, il est possible de se demander si l'utilisation de caméras de surveillance est réellement efficace et s'il permet véritablement de diminuer la vulnérabilité des infrastructures essentielles. Trois inconvénients principaux peuvent être soulevés. Le premier est que même si le contrôle des personnes peut éventuellement être efficace contre les actes terroristes, il ne permettra pas de se prémunir face à d'autres types d'aléas (naturel ou technique). Deuxièmement, le fait de filmer des endroits stratégiques en permanence induit une quantité très importante d'information à traiter. Troisièmement, le développement de la surveillance s'est fait sans véritablement intégrer comment l'information ainsi obtenue pourrait être utilisée devant les tribunaux (Radio Canada, 2008).

Parallèlement au programme CONTEST, le *London Resilience Partenership* a permis de développer la résilience de la ville de Londres en développant des plans de mesures d'urgence et de continuité opérationnelle. Ces plans ont permis de réagir plus rapidement lors des attentats de juillet 2005. Après la problématique terroriste, ce partenariat, regroupant divers organismes gouvernementaux et propriétaires d'infrastructures essentielles, étudie actuellement les moyens de répondre adéquatement à différentes menaces pouvant affecter la capitale britannique. Les menaces étudiées sont les pandémies (grippe aviaire), les évacuations à grande échelle et les problèmes climatiques. Ce partenariat a également mené à la constitution du site Internet de la *London Resilience Team* qui permet au public d'obtenir de l'information et du soutien en ce qui concerne les mesures d'urgence et la continuité opérationnelle (London Resilience Team, 2008).

De manière plus spécifique pour les infrastructures essentielles, le *Centre for the Protection of National Infrastructure* (CPNI) a été créé en février 2007. Ce centre intergouvernemental est formé de la réunion du *National Infrastructure Security Coordination Centre* (NISCC), du *United Kingdom's Security Service* (MI5) et du *National Security Advice Centre* (NSAC). Le NISCC se focalisait sur la sécurité informatique et les questions d'assurance de l'information tandis que le NSAC travaillait sur la sécurité physique et du personnel des infrastructures essentielles.

Le CPNI a pour objectif de fournir des conseils de sécurité pour les infrastructures essentielles dans le cadre de la stratégie gouvernementale pour améliorer la sécurité nationale. Pour cela, il utilise les ressources du MI5, du *Communications Electronics Security Group* (CESG), du *United Kingdom National Technical Authority for Information Assurance* et d'autres départements responsables de la sécurité des infrastructures essentielles (CPNI, 2008).

Même si les conseils du CPNI concernent l'amélioration de la sécurité des infrastructures essentielles face à l'ensemble des aléas pouvant affecter les

infrastructures essentielles, les travaux actuels portent presque exclusivement sur la menace terroriste.

Cela transparait au niveau de la considération du risque cybernétique ou de la vulnérabilité des infrastructures essentielles face aux éléments cybernétiques. En effet, l'élément cybernétique est considéré du point de vue de la protection ou du renforcement face à des attaques informatiques. Actuellement, la problématique de la vulnérabilité des infrastructures essentielles engendrée par la dépendance face à l'utilisation d'information (données) ne semble pas abordée à tout le moins par les organismes gouvernementaux britanniques qui s'intéressent aux infrastructures essentielles.

1.1.2.3.2 Travaux en France

En France, comme en Grande-Bretagne, la considération des risques pour les infrastructures essentielles se développe essentiellement en raison d'une préoccupation croissante pour la protection des infrastructures essentielles face au terrorisme.

L'ensemble de la sécurité civile qui gère les risques est de la responsabilité du ministère de l'Intérieur et du ministère de l'Écologie, de l'Énergie, du Développement durable et de l'Aménagement du territoire avec les lois du 30 juillet 2003 portant sur la prévention des risques technologiques et naturels et à la réparation des dommages ainsi qu'à celle du 13 août 2004 modernisant la sécurité civile. De manière générale, les risques technologiques étudiés concernent essentiellement les industries chimiques avec les installations classées et la directive Seveso II (MEEDA, 2008b).

La protection des infrastructures essentielles ou infrastructures vitales est sous la responsabilité du Secrétariat général de la défense nationale (Lasbordes, 2006). L'État a la responsabilité, en relation avec les représentants des secteurs

stratégiques économiques, de la protection des infrastructures vitales. Cette protection s'articule essentiellement autour de la problématique terroriste.

La France définit donc des infrastructures vitales qui sont des systèmes ou des réseaux constitués d'éléments humains, matériels et immatériels, indispensables à la production ou à la circulation de biens ou de services destinés à assurer les besoins prioritaires de la vie individuelle, collective, économique et sociale des citoyens et le fonctionnement régulier des pouvoirs publics (Lasbordes, 2006).

Les principales infrastructures vitales sont l'énergie électrique, les télécommunications, les transports, la chaîne de transactions interbancaires, le réseau de vigilance sanitaire, la chaîne des prestations sociales et la distribution d'eau potable (Lasbordes, 2006).

Elle définit également des secteurs d'activités d'importance vitale. Ces secteurs sont les activités ayant trait à la production et la distribution de biens ou de services indispensables à la satisfaction des besoins essentiels pour la vie des populations, à l'exercice de l'autorité de l'État, au fonctionnement de l'économie, au maintien du potentiel de défense et à la sécurité de la Nation, dès lors que ces activités sont difficilement substituables ou remplaçables, ou peuvent causer un danger grave pour la population (Lasbordes, 2006).

Ce concept d'activités vitales est particulièrement intéressant dans le sens où il fait référence aux besoins de la société qui peuvent être satisfaits par les infrastructures essentielles. Il peut également être appliqué aux infrastructures essentielles qui peuvent être définies comme des utilisatrices et des fournisseuses de ressources pour satisfaire leurs besoins ou remplir leurs missions.

La France a réellement commencé à se préoccuper de la protection des infrastructures essentielles en 2003 dans un contexte de défense nationale et de continuité de l'état (Viellard et Ribnikar, 2003). Il s'agissait de déterminer les

infrastructures essentielles qui pourraient s'avérer être des cibles stratégiques de manière à définir leur niveau de protection et l'affectation possible de la société.

L'étude réalisée par la compagnie européenne d'intelligence stratégique a montré que certaines infrastructures essentielles n'avaient pas réellement pris en compte leur degré de vulnérabilité face à un acte terroriste et n'avait par conséquent pas mis en place de mesure de protection appropriée (Viellard et Ribnikar, 2003). De plus, même si les risques reliés aux infrastructures essentielles sont connus au cas par cas, ceux découlant de leurs interdépendances n'étaient pas encore connus en 2003. L'étude réalisée par Viellard et Ribnikar (2003) montre donc la nécessité de considérer la protection des infrastructures essentielles prise dans leur ensemble et non indépendamment les unes des autres. De plus, une prise de conscience de l'ensemble de l'appareil étatique s'avérait nécessaire de manière à développer des processus de sensibilisation et d'entraînement à la gestion de crise impliquant les infrastructures essentielles (Viellard et Ribnikar, 2003).

En 2003, c'est donc une vision politique et économique qui prédomine en France pour la protection des infrastructures essentielles. Il s'agit donc plus de se prémunir face aux menaces qui pourraient influer sur le fonctionnement de l'état que d'analyser la continuité opérationnelle des infrastructures essentielles. Ceci s'explique certainement de par le fait que les infrastructures essentielles sont responsables de mener leur propre processus de gestion des risques de façon à assurer leur continuité opérationnelle. La préoccupation de l'état intervient lorsque la défaillance d'une de ces infrastructures pourrait affecter l'ensemble ou une partie de la société. Les travaux de Viellard et Ribnikar (2003) mettent donc l'emphase sur la nécessité de développer des exercices de simulation basés sur des scénarios de manière à entraîner les décideurs à conduire une gestion de crise reliée à la défaillance d'une infrastructure essentielle.

L'approche générale française favorise une vision stratégique plutôt que véritablement opérationnelle de la protection des infrastructures essentielles. Elle est plus axée sur une approche de sécurité que de sûreté de fonctionnement.

Cela se traduit au niveau de la vulnérabilité cybernétique des infrastructures essentielles par la prise en compte de la protection des infrastructures face à des cyberattaques et donc par le renforcement des réseaux face aux risques informatiques. La continuité opérationnelle des infrastructures essentielles abordant la problématique de la qualité de service et de la qualité de fonctionnement pouvant être altérées par la dégradation de données ne semblent pas prises en compte.

Toutefois, des travaux plus opérationnels se développent également. Il est possible de mentionner en particulier les travaux réalisés par MIBS Infrastructure & Services et ceux de l'institut national des hautes études de sécurité (INHES).

Le MIBS Infrastructure & Services travaille dans le domaine de la sécurité informatique. Il montre notamment l'aspect critique des infrastructures informatiques du fait de l'importance des systèmes d'information des entreprises et des infrastructures essentielles (MIBS, 2006). Il s'agit de développer des plans de reprises des activités de manière à favoriser l'adaptabilité des systèmes d'information de manière à rendre les entreprises les moins vulnérables possible. Une fois encore, la problématique cybernétique est essentiellement abordée en considérant la protection des infrastructures essentielles face à des actes malveillants.

Les travaux de l'institut national des hautes études de sécurité portent sur la sécurité économique et la gestion de crise. Ils ont pour but de mieux connaître les risques en favorisant un approfondissement de la connaissance et en analysant les nouveaux risques (INHS, 2008a).

L'INHES assure également le secrétariat du conseil national de sécurité civile qui a pour mission d'apporter aux pouvoirs publics, des avis relatifs à la prévention, la veille, l'alerte, la protection des populations, la gestion des crises et l'information du public (INHS, 2008a). L'INHES intervient donc au premier plan en ce qui a trait à la gestion des risques. Cependant, actuellement peu de travaux se focalisent sur les infrastructures essentielles.

En 2008, l'INHES a lancé un appel à proposition de recherche portant notamment sur la protection des infrastructures vitales dans un contexte de défense civile. Cet appel à proposition de recherche s'explique par le nombre croissant d'infrastructures à protéger, la nature et le niveau des menaces (menaces terroristes, catastrophes naturelles, accident technologique, etc.).

Il faut considérer l'interdépendance et la vulnérabilité croissantes des États en considérants la protection de plus en plus à l'échelle européenne, voire internationale. Il faut également définir ce que sont les infrastructures vitales ou plus exactement les activités vitales et définir l'application du cadre législatif existant (INHES, 2008b).

Un autre programme de financement a été lancé en France en 2008 en ce qui concerne la protection des infrastructures essentielles. Il s'agit du programme concepts, systèmes et outils pour la sécurité globale (CSOSG) qui est supervisé par l'Agence Nationale de la Recherche en partenariat avec la Délégation générale pour l'Armement et la Direction générale de la Police nationale (Agence Nationale de la Recherche, 2008).

Suite à une première liste de priorités nationales de recherche en sécurité établie en 2006, le programme de recherche CSOSG vise à améliorer la sécurité globale du pays. La sécurité globale correspond à assurer à la société un niveau suffisant de prévention et de protection contre les risques de toutes natures et de tous impacts

dans des conditions qui favorisent le développement sans rupture de la vie et des activités collectives et individuelles (Agence Nationale de la Recherche, 2008).

Le programme CSOSG a pour objectif le développement d'une approche systémique considérant les vulnérabilités et les interdépendances des systèmes complexes. Pour cela, le programme définit quatre (4) axes de recherche :

- la sécurité des citoyens ;
- la protection des infrastructures vitales, des réseaux et de leurs interconnexions ;
- la gestion de crise ;
- la sécurité aux frontières.

La protection des infrastructures vitales vise l'atteinte de solution découlant d'une approche systémique intégrant les avancées technologiques et favorisant les partenariats entre les divers acteurs publics et privés du domaine. Même si les projets devront favoriser une approche tous risques, une importance particulière est donnée aux aléas externes et en particulier aux actes de malveillance.

Les travaux français sont donc encore à un état embryonnaire et il n'y a encore que peu de résultats concrets ou de développement de méthodes d'analyse de vulnérabilités des infrastructures essentielles.

1.1.2.3.3 Travaux aux Pays-Bas

Parmi les travaux effectués en Europe, ceux des Pays-Bas se démarquent de par leur rôle de précurseur et par leur degré d'avancement. De plus, ils abordent la protection des infrastructures essentielles de manière plus globale que les travaux français ou britanniques. Les travaux néerlandais de protection des infrastructures essentielles ont véritablement débuté en 2002 avec la mise en œuvre du programme *« Besherming vitale infrastructuur »* (Luiijf et coll., 2003).

Ce programme est subdivisé en plusieurs étapes. La première étape a consisté à faire une sorte d'état des lieux (Quick scan) en déterminant les infrastructures essentielles présentes aux Pays-Bas et en évaluant leur degré de préparation (vulnérabilité et mesures de protection) face à différents aléas (la considération du terrorisme étant privilégiée) dans une approche voulant analyser tous les risques et considérant les notions d'interdépendances directes et géographiques de premier et de second ordre (Luiijf et coll., 2003). Pour effectuer cet état des lieux, ils se sont interrogés à savoir quelles infrastructures étaient essentielles ou critiques en essayant de déterminer lesquelles fournissaient un produit ou un service vital pour le fonctionnement du pays dans sa globalité. Par la suite, ils ont utilisé des questionnaires envoyés aux gestionnaires d'infrastructures essentielles pour déterminer les dépendances, interdépendances et l'état de préparation face à différents aléas avec une prépondérance pour l'aléa humain de type violation (actes de sabotage) (Reason, 1993). Pour effectuer ces analyses de risques, aucune méthode particulière n'était spécifiée. Le choix d'une méthode était laissé libre aux responsables de chacune des infrastructures essentielles considérées dans l'étude.

Les travaux néerlandais ne semblent pas aborder de manière spécifique la problématique de la cybernétique. Ils semblent plutôt se focaliser sur les dépendances et interdépendances physiques entre infrastructures essentielles.

Les travaux néerlandais ont montré la nécessité d'une approche encore plus globale de la protection des infrastructures essentielles en effectuant des travaux communautaires. Les travaux de l'Union européenne et de l'Organisation du traité de l'Atlantique nord se développent depuis les dernières années afin de répondre à ce besoin.

1.1.2.3.4 Travaux de la commission des communautés européennes

Les travaux de la commission ont débuté en juin 2004 suite à une demande du Conseil européen d'élaborer une stratégie globale de renforcement de la protection des infrastructures critiques. La même année, la commission a adopté une

communication intitulée « Protection des infrastructures critiques dans le cadre de la lutte contre le terrorisme » (Europa, 2008).

Pour répondre à cette demande, la commission a proposé un programme européen de protection des infrastructures critiques (PEPIC) et un réseau d'alerte concernant les infrastructures critiques, le Critical Infrastructure Warning Information Network (CIWIN) (Europa, 2008). Cette proposition a été acceptée en décembre 2004 (Europa, 2008).

L'objectif du PEPIC est de garantir des niveaux de sûreté suffisants et uniformes des infrastructures critiques, de réduire au minimum les défaillances et de fournir, pour l'ensemble de l'Union européenne, des moyens de réaction rapide (Commission des communautés européennes, 2005).

Le CIWIN est un réseau qui permettrait l'échange sécurisé des meilleures pratiques en servant de moyen de transmission des alertes et des informations sur les menaces (Commission des communautés européennes, 2005).
En juin et septembre 2005, deux séminaires sur la protection des infrastructures critiques de l'Union européenne se sont déroulés. Ces séminaires ont permis de faire connaître la manière dont les États membres abordaient la protection des infrastructures critiques (PIC). Il a également été décidé de publier un livre vert sur un programme européen de protection des infrastructures critiques décrivant les différents scénarios envisageables pour le PEPIC. Ce livre a été adopté par la commission en novembre 2005 (Commission des communautés européennes, 2005).

L'objectif premier du livre vert est de compiler les réactions des acteurs concernés face aux différents scénarios envisageables pour mettre en place le PEPIC, le CIWIN et l'établissement d'un programme européen de protection des infrastructures critiques.

Le livre vert présente cinq (5) éléments importants concernant les infrastructures essentielles (Commission des communautés européennes, 2005) :

- les risques que le PEPIC devrait aborder.

  Il s'agit de déterminer l'approche à privilégier d'une approche tous risques à une approche axée sur le risque terroriste.
- la responsabilité de l'Union européenne pour les infrastructures critiques européennes (ICE).

  Les ICE sont définies comme les infrastructures essentielles pouvant générer des effets transfrontières sur plusieurs États membres. Il est donc de la responsabilité de l'Union européenne de s'assurer de leur protection.
- la nécessité de prise en compte des interdépendances entre infrastructures essentielles.

  Il s'agit d'analyser les interdépendances entre infrastructures critiques, mais également au sein de ces infrastructures.
- la nécessité d'avoir une législation commune pour les infrastructures critiques nationales.

  Chaque État membre doit protéger ses infrastructures critiques nationales (ICN) en respectant un cadre commun de manière à éviter que les propriétaires et les exploitants de toute l'Europe soient soumis à des cadres différents et donc à une multitude de méthodologies et des surcoûts.
- la mise en œuvre d'un plan de sûreté pour les exploitants.

  Ce plan permettrait de recenser les actifs des infrastructures critiques et de définir les mesures de sûreté à mettre en œuvre pour leur protection.

Le livre vert présente également les sources de financement qui pourraient supporter les activités liées à la protection des infrastructures essentielles en Europe par l'entremise du programme « Prévention, préparation et gestion des conséquences en matière de terrorisme » (Commission des communautés européennes, 2005).

En 2006, une proposition de directive du conseil pose les bases de travail concernant le classement des ICE et la nécessité d'améliorer leur protection. Cette directive définit onze secteurs d'infrastructures critiques :

- Énergie ;
- Industrie nucléaire ;
- Technologies de l'information et des communications ;
- Eau ;
- Alimentation ;
- Santé ;
- Finance ;
- Transports ;
- Industrie chimique ;
- Espace ;
- Installations de recherche.

La directive répond aux interrogations du livre vert et définit une procédure de recensement et de classement des infrastructures critiques européennes ainsi qu'une approche commune pour évaluer la nécessité d'améliorer leur protection (Commission des communautés européennes, 2006a). La directive préconise que le PEPIC se base sur une approche tous risques conjuguée avec une priorité donnée au risque terroriste. La responsabilité de la protection des infrastructures essentielles demeure aux États membres et aux gestionnaires de ces réseaux. En effet, de nombreux États membres préparent leur propre approche en matière de protection des infrastructures critiques et attendent que la commission propose un programme global européen de protection de manière à pouvoir intégrer l'approche commune de l'Union. De ce fait, des mesures sont développées de manière à favoriser la communication entre les propriétaires et les États, mais aussi entre les États et la commission. Cette communication doit se faire dans un climat de confiance et de sécurité (Commission des communautés européennes, 2006a). En effet, une approche strictement nationale s'avère insuffisante pour permettre la protection des infrastructures essentielles. Ceci s'explique, car le faible niveau de

protection des infrastructures critiques dans certains États membres peut accentuer le niveau de vulnérabilité des autres États membres (Commission des communautés européennes, 2006a). Il suffit de penser aux gazoducs permettant d'alimenter l'Europe de l'ouest et traversant de nombreux États de l'Union européenne.

La directive définit six principes qui seront à la base de la mise en œuvre du PEPIC (Commission des communautés européennes, 2006b) :

1. subsidiarité : les efforts doivent porter sur les infrastructures revêtant un caractère critique sur le plan européen, plutôt que national ou régional ;
2. complémentarité : il faut éviter de dupliquer les efforts déjà consentis au niveau de l'Union européenne, des États et des régions ;
3. confidentialité : les informations sur la protection des infrastructures critiques doivent être classifiées et communiquées en cas de besoin ;
4. coopération des acteurs concernés : tous les acteurs concernés devront être associés autant que possible dès la mise en œuvre du PEPIC ;
5. proportionnalité : Des mesures ne seront proposées que lorsqu'un besoin aura été recensé par suite d'une analyse des failles en matière de sûreté et elles seront proportionnées au niveau de risque et au type de menace concerné ;
6. approche sectorielle : le PEPIC doit être conçu secteur par secteur et mis en œuvre en fonction d'une liste de secteurs d'infrastructures critiques ayant fait l'objet d'un accord.

Pour mettre en place le PEPIC, la Commission préconise une approche stratégique basée sur des actions à la fois contraignantes et non contraignantes. Il s'agit en effet de recenser les infrastructures essentielles et de définir leurs vulnérabilités tout en laissant le choix de la méthodologie employée à chacun des États membres (Commission des communautés européennes, 2006c).

Suite à la directive, la Commission a lancé un projet pilote comportant des actions préparatoires pour renforcer la lutte contre le terrorisme. Ce projet comportait un

programme pour l'amélioration de la protection des infrastructures essentielles visant à soutenir le PEPIC. L'objectif de ce programme était de définir et d'élaborer des mesures de protection des infrastructures essentielles par la mise au point de l'amélioration de méthodologies (Europa, 2008).

En janvier 2007, la proposition de directive du conseil concernant le recensement et le classement des infrastructures critiques européennes était encore en phase de consultation notamment auprès de la banque centrale européenne (Papademos, 2007).

En 2007, la Commission a également lancé un appel de propositions comportant les six thèmes suivants (Commission des communautés européennes, 2007) :

1. le renforcement des mesures de protection des infrastructures critiques ;
2. les points faibles et la capacité de résistance des infrastructures critiques ;
3. les stratégies d'atténuation et d'évaluation des risques pour les infrastructures critiques ;
4. la mise au point de plans d'urgence ;
5. la mise au point de normes communes de sécurité et de technologies innovantes pour la protection des infrastructures critiques ;
6. les projets transnationaux associant des partenaires dans au moins deux États membres ou au moins un État membre et un pays candidat.

De manière plus générale, les préoccupations concernant les infrastructures essentielles, au niveau européen, s'intègrent dans la stratégie européenne de sécurité adoptée par le Conseil européen en 2003 (Agence Nationale de la Recherche, 2008). Cette stratégie vise l'atteinte d'une sécurité globale à l'échelle européenne favorisant un traitement systémique et transversal de la sécurité.

Les préoccupations de l'Union européenne concernent donc essentiellement une approche stratégique et sectorielle de la protection des infrastructures critiques. L'emphase est mise sur la protection face aux actes terroristes. Actuellement, les

discussions sont encore en cours pour poser les bases d'un cadre commun et aucune application concrète ne semble avoir été développée. L'approche de l'Europe ne semble considérer, pour le moment, que les interdépendances résultant des liens physiques entre infrastructures essentielles. Les liens cybernétiques ne sont pas encore abordés. Toutefois, il est évident que la problématique cybernétique est considérée du point de vue de la protection face aux cyberattaques ceci par l'entremise des programmes de protection face aux risques informatiques.

1.1.2.4 Approche de l'Organisation du traité de l'Atlantique nord (OTAN)

A priori, la protection des infrastructures essentielles ne fait pas partie du domaine de compétence de l'OTAN. Cependant, elle s'est intéressée à cette question dès 2001 lorsqu'elle a effectué le bilan de l'état de préparation de ses membres en termes de planification et cartographie des infrastructures (OTAN, 2007).

Les activités que mène l'OTAN dans ce domaine s'inscrivent dans le cadre plus large du Plan d'action pour les plans civils d'urgence relatif à la protection des populations civiles face aux accidents chimiques, biologiques, radiologiques et nucléaires (CBRN), axé pour l'essentiel sur le terrorisme CBRN (OTAN, 2007).

En 2007, les travaux de la commission de la défense et de la sécurité de l'Organisation du traité de l'Atlantique nord présentent un état des connaissances dans le domaine de la protection des infrastructures essentielles en recensant les approches privilégiées par les États membres. Ils présentent également l'approche que devrait adopter l'OTAN dans ce domaine.

Pour l'OTAN, il s'agit de distinguer clairement les composantes des infrastructures qui sont critiques à l'échelon national de celles qui n'exigeraient pas d'intervention centralisée au niveau international (OTAN, 2007).

Pour cela, l'OTAN propose une démarche d'évaluation des risques en trois étapes :

1. recenser les menaces, identifier celles qui doivent faire l'objet de mesures et évaluer la probabilité de leur survenance.

   L'OTAN souligne qu'actuellement la priorité pour de nombreux États européens va à la protection face au terrorisme.
2. évaluer la vulnérabilité des infrastructures critiques en dressant le bilan de leurs points faibles.

   L'étude de la vulnérabilité soulève cependant des éléments qu'il faudra aborder : instances chargées de réaliser l'évaluation de la vulnérabilité, harmonisation de la méthodologie, utilisation de normes communes, supervision de la mise en œuvre de la méthodologie.
3. évaluer les conséquences sur une infrastructure de la concrétisation éventuelle d'une menace donnée.

   La notion de conséquences intègre donc les questions d'interdépendances intrasectorielles, mais également transversales entre infrastructures essentielles. Comme le soulignent les travaux de la commission, une cyberattaque grave n'affectera pas seulement une infrastructure informatique, mais se fera ressentir sur l'ensemble des infrastructures utilisant les réseaux informatiques.

La troisième étape est primordiale, car les interdépendances sont encore bien mal connues et les informations nécessaires ne sont pas forcément disponibles. De plus, les politiques de protection des infrastructures critiques tant nationales qu'internationales commencent à peine à aborder cette problématique (OTAN, 2007).

La commission de la défense et de la sécurité de l'OTAN se pose également la question de la responsabilité de la protection des infrastructures essentielles. La protection de ces infrastructures demeure de la responsabilité des pays dans lesquels elles sont implantées. Toutefois, cela nécessite un partenariat entre les pouvoirs publics et les exploitants d'infrastructures essentielles.

Actuellement, les États se focalisent principalement sur les éléments suivants (OTAN, 2007) :

- l'intégration de la protection des infrastructures essentielles dans le cadre des stratégies et politiques de protection civile/contre-terrorisme/sécurité intérieure ;
- la recherche et le partage de l'information sur les menaces ;
- la mise en place de dispositions destinées à assurer que les évaluations des risques effectuées par les exploitants sont réalisées suivant des procédures harmonisées, comparables et efficaces ;
- la formulation d'avis et d'orientations sur les mesures à prendre par les exploitants d'infrastructures essentielles pour protéger leurs installations ;
- la mise en place de mesures spécifiques destinées à assurer la prise en compte des interdépendances intrasectorielles et transversales ;
- le renforcement des mesures de protection ;
- la sensibilisation à la nécessité de la protection des infrastructures critiques et information du secteur commercial et de la population dans son ensemble ;
- l'apport d'aide financière à l'appui des activités de protection, le financement de la recherche et de la mise en œuvre des technologies de protection.

Ces préoccupations sont essentiellement d'ordre stratégique. Ceci s'explique par le fait que la sécurité des réseaux demeure de la responsabilité de leurs gestionnaires. Toutefois, les États doivent intervenir dans la protection des infrastructures critiques puisque les gestionnaires d'infrastructures essentielles ne peuvent en aucun cas assurer seuls les conséquences financières sur la société civile qu'engendrerait la défaillance de leurs réseaux. De plus, il faut également régler le problème du partage de l'information. En effet, les gestionnaires de réseaux peuvent être réticents à fournir de l'information sur leurs vulnérabilités ce qui pourrait constituer un avantage pour leurs concurrents.

La communication est un élément prépondérant de la gestion des risques. En effet, la protection des infrastructures critiques concerne avant tout les installations plutôt

que les personnes. Cependant, son objectif ultime reste la protection des populations via des mesures destinées à assurer le maintien en fonctionnement des services essentiels. L'information et l'implication du public sont donc des aspects déterminants, qui occupent habituellement une place importante dans les politiques de protection nationales (OTAN, 2007).

L'approche de l'OTAN se démarque de l'approche de l'Union européenne, car elle ne cherche pas à réglementer la protection des infrastructures critiques. Les programmes de l'OTAN visent plus la promotion de normes plus poussées en matière de préparation des États. Ils cherchent donc à renforcer l'interopérabilité dans le cadre de la gestion des conséquences et à améliorer la résilience des infrastructures essentielles et donc des pays dans lesquels elles se trouvent (OTAN, 2007).

L'approche de l'OTAN est stratégique et en ce sens, elle n'aborde pas de manière spécifique des types de risques ou de vulnérabilités. La détermination des risques et des vulnérabilités demeurent de la responsabilité des États membres ou des infrastructures essentielles elles-mêmes. L'OTAN ne préconise donc pas de méthode d'analyse des vulnérabilités cybernétiques d'une infrastructure essentielle.

Maintenant que nous avons vu ce qui se fait au niveau international, tout du moins à partir des résultats publiés, il est important de regarder quels travaux se font actuellement au Canada pour la protection des infrastructures essentielles.

1.1.2.5 Travaux au Canada

L'approche du Canada préconise d'assurer la protection et la sécurité de ses citoyens. Il s'agit de s'assurer que le gouvernement soit préparé à faire face aux menaces présentes et futures, et qu'il puisse y répondre. Pour cela, le Canada a mis en place une politique de sécurité nationale. Cette politique met l'accent sur des événements et des circonstances qui exigent généralement une réaction nationale

parce que les individus, les collectivités ou les provinces n'ont pas la capacité d'y faire face par leurs propres moyens (SPC, 2008a).

En ce qui concerne la gestion des risques associés aux infrastructures essentielles, les travaux ont véritablement débuté en octobre 1998 avec la constitution du Groupe de planification nationale des contingences (GPNC), Le GPNC avait pour but de produire une évaluation des risques pour les infrastructures nationales. Le but de cette évaluation était de faciliter le passage à l'an 2000 en déterminant les infrastructures à risque et en évaluant leur possibilité de défaillances. Après le nouveau millénaire, l'ensemble des travaux du GPNC a été repris par la Critical Infrastructure Protection Task Force (CIPTF). Depuis février 2001, la CIPTF fait partie intégrante du Bureau de la Protection des Infrastructures essentielles et de la Protection civile (BPIEPC) intégré au sein de SPC. Les travaux du GPNC ont mené à la publication en mars 2000 d'un rapport portant sur les dépendances qui existent entre les infrastructures canadiennes et les vulnérabilités que cela induit (NCPG, 2000).

Pour cela, les dépendances entre un réseau A et un réseau B sont caractérisées suivant une échelle à quatre (4) degrés :

- **0 :** l'infrastructure A ne dépend pas de l'infrastructure B dans le sens où la défaillance de l'infrastructure B n'affectera pas l'infrastructure A ;
- **1 :** l'infrastructure A est faiblement dépendante de l'infrastructure B dans le sens où la défaillance de l'infrastructure B entraînera des interruptions de service mineures de l'infrastructure A ;
- **3 :** l'infrastructure A est moyennement dépendante de l'infrastructure B dans le sens où la défaillance de l'infrastructure B entraînera des interruptions de service notables de l'infrastructure A, de même que des dégradations potentielles ;
- **9 :** l'infrastructure A est fortement dépendante de l'infrastructure B dans le sens où la défaillance de l'infrastructure B entraînera l'arrêt de fonctionnement de l'infrastructure A.

Les résultats sont présentés sous forme d'une matrice à double lecture. De gauche à droite, la matrice définit la vulnérabilité d'une infrastructure sur une autre. De haut en bas, la matrice définit l'impact d'un réseau par rapport à un autre (Tableau 1.2). Cette présentation sous forme de matrice permet une lecture facile et rapide des résultats obtenus lors de cette étude. La matrice se lit dans les deux sens. Ce mode de représentation a également l'avantage de reprendre le système de classification qui a été utilisé pour la détermination des degrés de dépendances (0, 1, 3 et 9) en le redéfinissant en termes de vulnérabilité.

Tableau 1.2 - Exemple de matrice de vulnérabilité et d'impact.

Réseau	A	B	C
A		H	
B	M		F
C	H	H	

H : haute dépendance ; M : dépendance moyenne ; F : faible dépendance ; case blanche : absence de dépendance.

Dans cet exemple, le réseau A est très dépendant du réseau B (H) mais il ne dépend pas du tout du réseau C. Le réseau B dépend peu du réseau C (F). Le réseau A a un impact moyen sur le réseau B (M) mais il a un impact élevé sur le réseau C (H). Le réseau B a un impact élevé sur le réseau C (H).

La vulnérabilité est définie ici comme une caractéristique de la conception, de la mise en marche ou de l'opération d'une infrastructure ce qui la rend sujette à la destruction ou à la diminution de fonctionnement par la survenue d'une menace. Cette vulnérabilité est définie suivant une échelle à quatre degrés :

- vulnérabilité nulle : cette vulnérabilité correspond à une infrastructure critique qui par conception, mise en œuvre, opération ou toutes combinaisons possibles n'a aucune possibilité d'être détruite ou affectée par une menace ;

- vulnérabilité faible : cette vulnérabilité correspond à une infrastructure critique qui par conception, mise en œuvre, opération ou toutes combinaisons possibles n'a qu'une faible possibilité d'être détruite ou affectée par une menace ;
- vulnérabilité moyenne : cette vulnérabilité correspond à une infrastructure critique qui par conception, mise en œuvre, opération ou toutes combinaisons possibles n'a qu'une possibilité moyenne d'être détruite ou affectée par une menace ;
- vulnérabilité forte : cette vulnérabilité correspond à une infrastructure critique qui par conception, mise en œuvre, opération ou toutes combinaisons possibles a une possibilité extrême d'être détruite ou affectée par une menace.

Les travaux du GPNC mènent donc à l'élaboration d'une matrice de dépendances similaire à celle présentée dans le tableau précédent (Tableau 1.2). Cette matrice a été réalisée à partir d'une analyse qui se veut exhaustive des différents types de réseaux et de leurs interactions. Toutefois, cette analyse de dépendances est souvent réalisée à partir de l'utilisation de scénarios ce qui peut conduire à identifier certaines interrelations, mais aussi à en oublier. Il n'y a pas d'approche systématique ni de considération locale ou spécifique à certains réseaux. D'autre part, les différentes problématiques soulevées dans chaque cas peuvent paraître assez subjectives puisqu'elles sont exclusivement basées sur une vision gouvernementale de la problématique. D'un autre côté, le découpage des différents réseaux est assez pertinent et les cas explorés, même s'ils ne résultent pas d'une classification applicable dans tous les cas, sont réalistes. Cependant, il est dommage, dans cette approche, que les réseaux de production d'eau potable et ceux de traitement des eaux usées ne soient pas pris en compte en tant que réseau propre. Les réseaux d'entraide et d'éducation sont également non considérés. En outre, il n'y a pas de réseaux spécifiques pour l'informatique et le gouvernement bien que leur implication apparaisse pour l'ensemble des réseaux étudiés. La problématique cybernétique n'est en ce sens pas abordée.

Ces travaux de recherche sur la vulnérabilité des infrastructures essentielles effectués en 2000 par le GPNC ne semblent pas avoir donné de suite. Cela ne veut pas dire que la problématique des interdépendances entre infrastructures essentielles ne demeurait pas importante au Canada, bien au contraire.

En avril 2004, le Canada par l'entremise de la Politique de sécurité nationale s'est doté d'une Stratégie nationale (SPC, 2008a) et d'un plan d'action pour la protection des infrastructures essentielles (SPC, 2008a).

Le plan d'action pour la protection des infrastructures essentielles se base sur cinq principes directeurs (SPC, 2008b) :

- la sensibilisation des gestionnaires des infrastructures essentielles à la nécessité de mettre en œuvre la protection des infrastructures essentielles (PIE) ;
- l'intégration de l'ensemble des subdivisions de la sécurité civile à savoir, la gestion des risques, les mesures d'urgence et la continuité opérationnelle ;
- la participation de l'ensemble des parties prenantes dans le domaine à la fois du secteur privé et du secteur gouvernemental ;
- la responsabilisation des partenaires (gestionnaires d'infrastructures essentielles) face à la société canadienne ;
- une approche tous risques tant technique, sociale que naturelle.

D'autres éléments, même s'ils ne constituent pas des principes, n'en demeurent pas moins primordiaux pour le développement d'une stratégie nationale de protection des infrastructures essentielles (SNPIE). Ce sont la prise en compte des vulnérabilités des infrastructures essentielles, les interdépendances entre infrastructures essentielles, les notions de communication des informations pertinentes et la prise en compte de la confidentialité des données ainsi que les notions de gouvernance et de partenariats internationaux (SPC, 2008c).

En 2008, le Canada vise à mettre en place une Stratégie nationale sur les infrastructures essentielles pour renforcer la résilience des infrastructures essentielles contre les dangers actuels et émergents.

La Stratégie prévoit que les propriétaires et les exploitants sont les premiers responsables de la protection des infrastructures essentielles. Les gouvernements fédéral, provinciaux et territoriaux participent également à la protection de leurs propres infrastructures essentielles et appuient les propriétaires privés.

Cette protection passe par une approche de gestion tous risques qui permettra de gérer et de faire connaître les menaces, les risques, les vulnérabilités et les interdépendances dans l'ensemble de la collectivité des infrastructures essentielles.

La stratégie prévoit renforcer la résilience des infrastructures essentielles en combinant :

- des mesures de sécurité pour s'occuper des menaces causées par l'homme ;
- des mesures de continuité opérationnelle visant à assurer les services essentiels ;
- des mesures de planification d'urgence.

Pour cela, il faut développer des partenariats en créant des réseaux sectoriels pour chacun des secteurs des infrastructures essentiels qui auront pour objectifs :

- l'échange et la protection des informations pertinentes en vertu de la loi sur la gestion des urgences ;
- la détermination des questions d'intérêt national, régional ou sectoriel ;
- l'utilisation des connaissances des experts des secteurs public et privé ;
- l'élaboration d'outils pour renforcer la résilience des infrastructures essentielles couvrant tous les aspects de la prévention, de la préparation, de l'intervention et du rétablissement.

La mise en œuvre de la Stratégie repose sur les capacités, les programmes et les ententes fédérales, provinciales, territoriales, du secteur public et du secteur privé, déjà en place. L'harmonisation de ces activités dans le cadre d'une approche cohérente est fondamentale à l'élaboration d'un programme national sur les infrastructures essentielles.

La mise en œuvre de la Stratégie nationale sur les infrastructures essentielles se fera suivant trois volets :

- partenariats ;
- gestion des risques ;
- échange d'information.

La Stratégie définit également les rôles des différents acteurs qui doivent être impliqués dans la protection des infrastructures essentielles (Tableau 1.3).

Au cours des deux premières années, les partenaires concentreront leurs efforts surtout sur l'établissement des réseaux sectoriels et la mise sur pied du Forum national intersectoriel, ainsi que sur l'amélioration du processus d'échange de l'information.

Au cours des années suivantes, l'efficacité des réseaux sectoriels et l'amélioration de l'échange de l'information permettront de mieux gérer les risques et de mettre en place des plans et des exercices de gestion des urgences.

Tableau 1.3 - Rôles et responsabilités des acteurs pour la protection des infrastructures essentielles (SPC, 2008d).

Intervenants	Rôles	Responsabilités
Gouvernement fédéral	Diriger des activités nationales	• Faire progresser l'approche nationale collective en matière de protection des infrastructures essentielles (IE) ; • Collaborer avec les associations nationales ; • Collaborer avec les propriétaires et les exploitants des IE dont les activités relèvent du champ de compétence fédérale, et ce, en consultation avec les provinces et les territoires.
Gouvernements provinciaux ou territoriaux	Diriger des activités provinciales ou territoriales	• Collaborer avec le gouvernement fédéral, les provinciaux ou provinciales ou provinces et les territoires pour atteindre les objectifs de la Stratégie nationale ; • Coordonner des activités avec d'autres ordres de gouvernement, dont des administrations locales, des associations, ainsi que des propriétaires et des exploitants d'IE.
Propriétaires et exploitants d'infrastructures essentielles	Gérer ensemble les risques liés à leurs infrastructures essentielles	• Assumer les responsabilités à l'égard de la gestion des risques ; • Participer aux activités de recensement des IE, d'évaluation, de prévention/atténuation, de préparation, d'intervention et de rétablissement.

Pour développer et opérationnaliser cette stratégie de protection des infrastructures essentielles, le Canada se base plus spécifiquement sur deux programmes (SPC, 2008b) :

- le programme national de fiabilité des infrastructures essentielles (PNFIE) ;
- le programme conjoint de recherche sur les interdépendances des infrastructures (PCRII).

Le PNFIE, élaboré en 2002, constitue la base du développement de la stratégie de protection des infrastructures essentielles. En effet, ce programme a été développé pour élaborer une approche commune de collaboration entre les gouvernements et les gestionnaires d'infrastructures essentielles dans le but de garantir le bon fonctionnement de ces infrastructures. En ce sens, il visait à instaurer le cadre et à raffiner les principes sous-tendant la SNPIE (Infrastructure Canada, 2008).

Le PCRII a été lancé en 2005, sous l'égide de Sécurité publique Canada (SPC) et du Conseil de recherches en sciences naturelles et en génie (CRSNG). Ce programme se terminant en février 2008 avait pour but de développer des connaissances et des pratiques scientifiques de manière à mieux gérer les risques reliés aux interactions entre infrastructures essentielles (SPC, 2008e). En ce sens, ce programme de recherche venait compléter les visées du PNFIE et en particulier la nécessité de développer les connaissances face aux interdépendances entre infrastructures essentielles (SPC, 2008e).

Ce programme a permis de financer six projets de recherche :

- la prise de décision pour les liens essentiels dans les réseaux d'infrastructures du Dr Jose Marti de l'Université de Colombie-Britannique ;
- modéliser les interdépendances pour la gestion des mesures d'urgence du Dr Vincent Tao de l'Université York ;
- méthodologie d'étude des interdépendances entre les réseaux de support à la vie du Dr Robert de l'École Polytechnique de Montréal ;

- mettre au point un modèle d'interdépendances des infrastructures du Dr Tamer El-Diraby de l'Université de Toronto ;
- simulation des réseaux d'infrastructures essentiels du Dr Wenjum Zhang de l'Université de Saskatchewan ;
- résilience des infrastructures d'alimentation d'eau et des systèmes d'urgence sanitaire aux maladies d'origine hydrique des Drs Edward McBean et Corinne Schuster de l'Université de Guelph.

Ces projets de recherche abordent la problématique des interdépendances entre infrastructures essentielles de manières très différentes. Cependant, certaines tendances se démarquent qui permettent de créer des classes de projets.

Les travaux de José Marti, de Wenjum Zhang et de Vincent Tao semblent vouloir favoriser le développement de modélisations informatiques. Le projet de José Marti vise à modéliser l'ensemble des interdépendances existantes entre différentes infrastructures essentielles présentes sur le site de l'université de Colombie-Britannique de manière à favoriser la gestion et la réponse aux situations d'urgence (Marti et coll., 2008). Le projet du Dr. Marti a donné lieu à la création d'un logiciel de simulation, *I2SM framework*, qui, en se basant sur des simulations de scénarios essentiellement d'origine naturelle et sur une modélisation mathématique de l'ensemble des infrastructures essentielles présentes dans un secteur donné, vise à anticiper les défaillances et à favoriser la mise en œuvre des étapes de préparation, prévention, intervention et rétablissement. L'équipe de recherche de l'université de Colombie-Britannique (*Infrastructure interdependencies Simulation Team*) vise dans de prochaines étapes à intégrer dans leur modèle les notions de facteur humain et la considération de la problématique cybernétique. Le modèle informatique développé est confronté à quelques difficultés. Pour être fonctionnel, il nécessite une grande quantité de données qui peuvent être difficiles à obtenir et à gérer, particulièrement en ce qui a trait à sa mise à jour. Il faut en effet prendre en compte l'évolution temporelle et le changement des informations nécessaires au bon fonctionnement du modèle, de même que la pertinence et le potentiel d'utilisation

du résultat obtenu. Cette grande quantité d'information à gérer engendre des risques de duplication de cette information. De plus, pour traiter cette information, il faut une base de données importante de même que les outils informatiques permettant de l'utiliser. Le modèle *I2SM framework* semble très efficace, mais se trouve donc limité par la lourdeur des données et du matériel nécessaires à son fonctionnement. Le projet de Wenjum Zhang vise également la modélisation des interdépendances, mais dans le but de favoriser le bon fonctionnement des réseaux et d'éviter leurs défaillances. Pour cela, il utilise les réseaux de pétri de manière à modéliser la complexité des relations existantes entre infrastructures essentielles (Zhang, 2008). Pour le moment, ce travail demeure très théorique et n'a pas donné lieu à des applications concrètes. Le dernier projet consistant à de la modélisation est celui de Vincent Tao qui utilise des systèmes de capteurs terrestres et de satellites qui combinés permettent de suivre en temps réel l'évolution d'un phénomène naturelle extrême (Cheng, 2008). L'outil développé permet en cela d'anticiper les infrastructures essentielles qui seront potentiellement affectées. Ceci, bien sûr, si leur localisation est connue. Toutefois, cet outil ne permet pas véritablement d'anticiper ou de visualiser les défaillances en cascades d'infrastructures essentielles en raison de leurs interdépendances.

Les travaux de Benoît Robert visent également l'analyse et l'évaluation des risques et des vulnérabilités reliés aux interdépendances entre infrastructures essentielles. Pour répondre à cette problématique, il s'agit de réaliser une étude exhaustive d'une infrastructure essentielle (Robert, 2001 ; Robert et coll., 2003a ; Petit et coll., 2004).

Contrairement aux autres projets de recherche présentés précédemment, ces travaux abordent la problématique en favorisant une approche déductive recentrée sur les conséquences et intégrant la prise en compte des besoins des infrastructures essentielles. Ils ne se focalisent pas uniquement sur les liens directs entre infrastructures essentielles, mais considèrent également les interactions géographiques qui sont prépondérantes en termes de mesures d'urgence (Robert,

2008). Ces travaux se démarquent également des autres projets de recherche, parrainés par le PCRII, par le nombre important de partenaires tant privés que gouvernementaux participants et par la volonté de développer un climat propice au partage des informations pertinentes à la gestion des risques. De plus, l'accent est mis sur l'aspect opérationnel des outils développés et sur leur appropriation par les personnes œuvrant dans le domaine des mesures d'urgence.

L'approche du *Centre risque & performance* (CRP) repose sur une caractérisation précise des missions d'une infrastructure essentielle, de ses modes d'opération et des infrastructures qui la composent (Robert et coll., 2003b ; Robert et coll., 2004a ; Robert et Petit, 2006).

Un réseau est fonctionnel lorsque l'ensemble de ses missions est rempli avec un degré d'efficience de 100 %. Dès qu'une mission n'est plus efficiente, le réseau entre en défaillance. Une défaillance découle d'une vulnérabilité du réseau, c'est-à-dire lorsqu'une opération et/ou une infrastructure n'est plus efficiente. L'ampleur de la vulnérabilité dépend de l'importance des éléments non efficients pour remplir la mission. Elle peut être analysée par le biais d'études de vulnérabilités qui permettront d'établir les éléments mis en cause (Robert et coll., 2004b ; Robert et coll. 2006).

Partant de ce constat, la méthode préconisée consiste donc à partir de la diminution d'efficience d'un système afin de remonter aux causes tout en intégrant les facteurs anthropiques et naturels. Le but n'est pas de déterminer la probabilité d'occurrence d'un événement, ce qui s'avère souvent imprécis, mais de définir la succession d'événements pouvant conduire à la défaillance d'un réseau. Il faut donc déterminer les conditions nécessaires pour atteindre un certain état, en tenant compte de l'arrivée d'aléas externes et de la diminution d'efficience de composantes du réseau (opération et infrastructures) (Petit et coll., 2004).

Pour cela, cette méthode vise à aborder la problématique de la vulnérabilité des infrastructures essentielles en se posant la question « Pourquoi ? » plutôt que « Et-Si ? ».

Les deux derniers projets de recherche à savoir les travaux de El-Diraby et ceux de McBean, bien qu'intéressants, ne semblent pas véritablement aborder la problématique des interdépendances entre infrastructures essentielles. Les travaux de El-Diraby visent le développement d'un langage commun et la représentation des connaissances concernant les infrastructures essentielles des points de vue technique et conceptuel. Pour ce faire, ce projet utilise les principes de l'ontologie qui vise à décrire les contraintes et les mécanismes sous-tendant les interactions des différents processus, acteurs et ressources (El-Diraby, 2007). Ce projet, bien que bien élaboré d'un point de vue théorique, se trouve relativement affaibli par le manque de partenaires gestionnaires d'infrastructures essentielles pouvant fournir des données pour nourrir le modèle développé. De plus, et pour la même raison, ce modèle ne semble pas permettre de répondre aux besoins des gestionnaires d'infrastructures essentielles. En effet, ici, l'outil a été développé avant de véritablement connaître la problématique à laquelle il devait répondre. Les travaux de McBean, quant à eux, visent l'analyse et la gestion d'une infrastructure essentielle particulière à savoir un réseau d'aqueduc. Ce projet est intéressant dans le sens où il se concentre sur la réponse aux maladies d'origine hydrique dans le but d'améliorer la résilience d'un réseau d'eau (McBean and Schuster, 2008). Toutefois, bien que très importante, cette problématique de la contamination de l'eau n'a pas de lien avec l'analyse des interdépendances entre infrastructures essentielles, tout du moins tel qu'abordé dans ce projet de recherche.

Les travaux et les programmes canadiens concernant les infrastructures essentielles n'abordent que très peu la problématique de la cybernétique. Il existe toutefois un organisme dédié à la cybersécurité des infrastructures essentielles. Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) est chargé de la surveillance des menaces et de la coordination des interventions aux incidents de

sécurité cybernétique. Son mandat est la protection des infrastructures essentielles contre les incidents cybernétiques (SPC, 2008f). Ce centre est plus particulièrement chargé :

- de la coordination et du soutien des interventions en cas d'incident ;
- de la surveillance et de l'analyse des menaces cybernétiques ;
- de la diffusion des conseils techniques sur la sécurité des technologies de l'information ;
- de la constitution de la capacité nationale (normes, pratiques exemplaires, sensibilisation, formation).

Les activités du CCRIC abordent donc la problématique cybernétique en termes de risque informatique et de protection face à des cyberattaques. Le CCRIC n'aborde pas la problématique cybernétique sous l'angle de la dépendance des infrastructures essentielles face à l'utilisation de données ou de la vulnérabilité des infrastructures essentielles face à la dégradation de ces données.

Comme nous venons de le voir, de nombreux travaux abordent la problématique des interdépendances entre infrastructures essentielles et des approches différentes sont développées. Il apparaît important de présenter, de manière synthétique, une comparaison entre ces différentes approches.

1.1.2.6 Comparaison des diverses approches

Cette revue de l'état de la connaissance dans le domaine des interrelations entre infrastructures essentielles et la prise en compte des effets domino montre que cette problématique est devenue une préoccupation mondiale.

Actuellement, la majorité des travaux sont basés sur des études inductives d'analyse de risques se basant sur des scénarios recentrés sur la probabilité d'apparition d'un aléa et la volonté d'avoir une approche globale permettant de modéliser l'ensemble des interdépendances pouvant exister entre tous les types d'infrastructures essentielles (De la Lande de Calan, 2007). Cette manière de procéder peut mener à

sous-estimer la vulnérabilité des infrastructures essentielles et par la même de la société en général. De plus, cette notion de vulnérabilité qui semble de plus en plus utilisée demeure assez floue. Il peut être assez difficile de différencier cette notion de celles de risque, d'aléas ou de conséquences.

Le tableau présenté en Annexe 1 montre également que la problématique cybernétique est peu ou pas abordée du point de vue de la sûreté des infrastructures essentielles et de leur dépendance face aux données. La problématique cybernétique est presque exclusivement abordée en termes de sécurité en considérant les actes de malveillance comme des aléas pouvant affecter les systèmes informatiques. De plus, le facteur humain qui est prépondérant dans un contexte de continuité opérationnelle n'est également que peu abordé.

Il est certainement difficile de considérer l'ensemble des interdépendances pouvant exister entre les infrastructures essentielles. Cependant, il apparaît important d'apporter une attention particulière à la dépendance des réseaux aux données qui sont nécessaires à leur opération et à leur contrôle. Dans ce contexte, il est utile de voir comment sont analysées les vulnérabilités engendrées par l'utilisation des systèmes de communication et des systèmes SCADA. Ces systèmes sont en effet particulièrement importants pour l'opération et le contrôle des infrastructures essentielles.

1.2 Système SCADA

Les systèmes SCADA correspondent à la technologie qui permet de collecter des informations d'unités distantes et de contrôler ces unités (Krutz, 2006). Ces systèmes de contrôle sont utilisés pour opérer les infrastructures essentielles. La sécurité en ligne des réseaux SCADA et des systèmes de gestion de processus est cruciale pour les infrastructures essentielles qui doivent s'assurer qu'il n'y a pas d'interruption de service, de réorientation des processus ou de manipulation des données opérationnelles pouvant entraîner de graves perturbations pour un pays (IBM, 2008).

Les vulnérabilités et la protection de ces systèmes de contrôle sont d'actualité. En effet, en Californie, un opérateur de l'acheminement d'eau du *Tehama Colusa Canal Authority* a été inculpé pour avoir installé illégalement du code sur le système SCADA dont il avait la charge. Cela a endommagé le système informatique et occasionné près de 5000 dollars de perte (McGregor, 2007).

En 2000, un cas analogue s'est produit en Australie à Nambour, au *Maroochy Water Services*. Un homme, après avoir accédé à l'infrastructure SCADA, a pu déverser les eaux d'égout dans des cours d'eau (Slay and Miller, 2008).

Plus récemment, c'est un adolescent de 14 ans qui a défrayé la chronique en concevant une télécommande capable de contrôler les aiguillages de la ville de Lodz en Pologne où il réside. Pour cela, le jeune garçon, connu pour sa passion de l'électronique, a modifié une simple télécommande de télévision (Leyden, 2008).

Ces événements montrent le besoin de renforcer la sécurité des systèmes de contrôle des infrastructures essentielles. Les systèmes critiques de contrôle en temps réel ont besoin d'être protégés par une solution de sécurité pouvant être adaptée en fonction des besoins spécifiques d'une industrie et d'une application, étant donné qu'une interruption de la sécurité du réseau de contrôle et des systèmes SCADA en temps réel est susceptible de suspendre les activités génératrices de revenus ou de provoquer des pannes importantes pour les infrastructures essentielles et la société civile (PR Newswire, 2008).

De plus, ces systèmes de commande et d'acquisition de données de surveillance sont maintenant connectés à des réseaux mondiaux. Leurs évolutions récentes font qu'ils nécessitent souvent un accès à Internet pour la visualisation, la commande et le contrôle à distance. Les nouveaux besoins en mobilité favorisent l'utilisation d'accès sans-fil. Tout cela fait qu'il est nécessaire de redéfinir en profondeur la sécurité des systèmes SCADA (Sécurité SCADA, 2008).

Depuis quelques années, les anciens protocoles propriétaires évoluent vers des protocoles standardisés, documentés et interconnectés pour chaque élément constituant les systèmes SCADA (Figure 1.2).

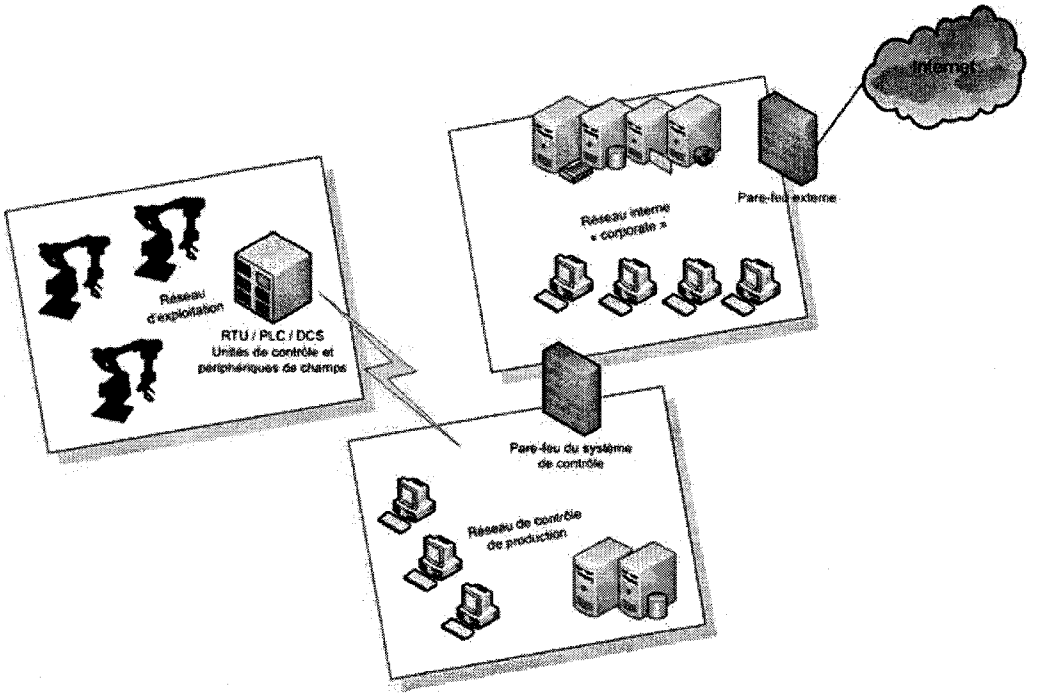

Figure 1.2 - Système SCADA (Sécurité SCADA, 2008).

En 2002, le *President's Critical Infrastructure Protection Board* et le *U.S. Department of Energy* ont défini un processus en 21 étapes permettant d'améliorer la cybersécurité des systèmes SCADA (OEA, 2002) (Figure 1.3) :

1. identifier toutes les connexions au réseau SCADA ;
2. déconnecter les connexions non nécessaires ;
3. évaluer et renforcer la sécurité des connexions restantes ;
4. renforcer les systèmes SCADA en enlevant ou en neutralisant les services non nécessaires ;
5. ne pas compter uniquement sur les protocoles internes pour protéger les systèmes SCADA ;
6. mettre en place les dispositifs de sécurité fournis par des services externes ;

7. établir des contrôles forts des éléments des systèmes SCADA pouvant servir de porte d'entrée ;
8. implémenter des systèmes de détection d'intrusion internes et externes et surveiller 24 heures sur 24 les incidents ;
9. effectuer des audits techniques du système SCADA et des réseaux reliés pour identifier les problèmes de sécurité ;
10. effectuer des enquêtes de la sécurité physique du système SCADA et des réseaux connectés ;
11. établir des équipes (*SCADA Red Teams*) pour identifier et évaluer des scénarios possibles d'attaques ;
12. définir clairement les rôles et les responsabilités des gestionnaires, administrateurs système et utilisateurs du système SCADA ;
13. documenter l'architecture réseau et identifier les systèmes servant aux fonctions critiques ou contenant de l'information sensible requérant des niveaux supplémentaires de protection ;
14. établir un processus rigoureux de gestion des risques ;
15. établir une stratégie de protection du réseau basée sur le principe de défense en profondeur ;
16. identifier clairement les besoins en cybersécurité ;
17. établir des processus de gestion effective de la configuration du système SCADA ;
18. effectuer des évaluations régulières du système SCADA ;
19. effectuer des copies de sauvegarde et développer des plans de rétablissement du système SCADA ;
20. établir des attentes précises pour les performances de cybersécurité et s'assurer que le personnel soit responsabilisé face à l'atteinte de ces niveaux ;
21. développer des politiques et effectuer des entraînements pour minimiser la possibilité que le personnel dévoile par inadvertance de l'information sensible en ce qui a trait à la conception, les opérations et les mesures de sécurité du système SCADA.

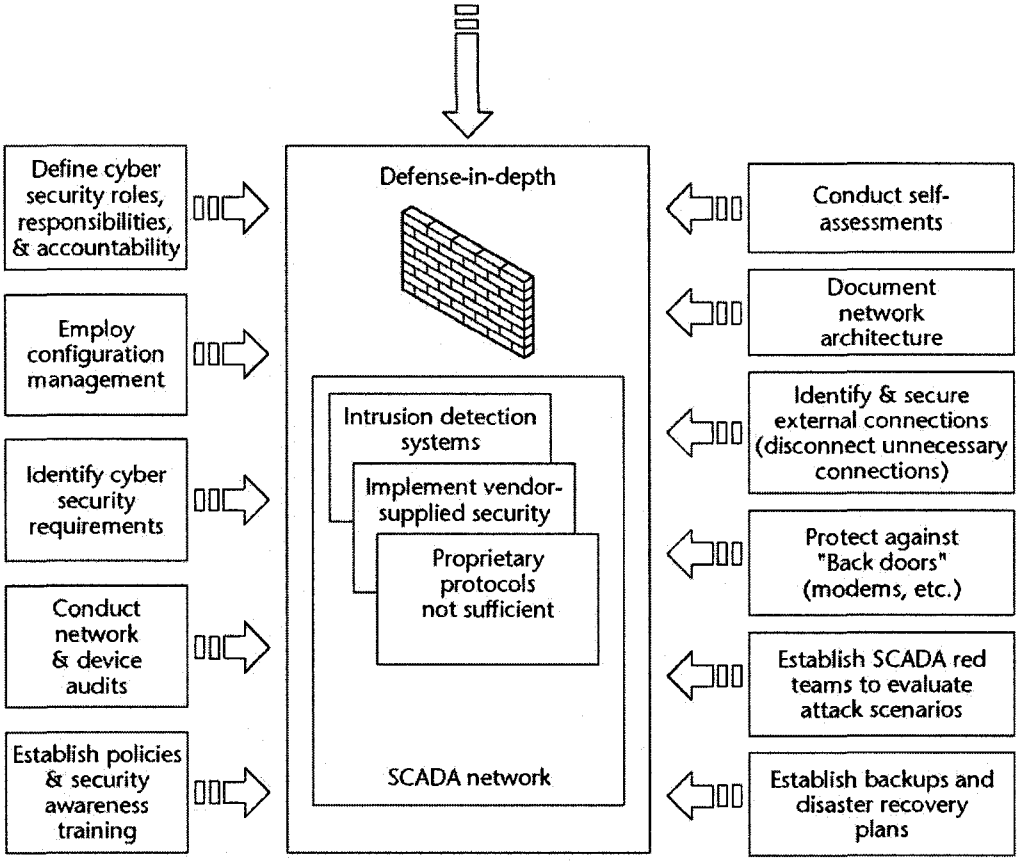

Figure 1.3 - Les étapes de la cybersécurité (OEA, 2002).

Le besoin de protection des systèmes SCADA est donc principalement pris en compte sous l'angle de la sécurité informatique. Des sociétés, telles que Verano, se sont spécialisées dans le développement de logiciel permettant de gérer la sécurité en temps réel de systèmes SCADA. Verano a conçu le logiciel *Industrial Defender* pour protéger contre toutes les formes d'agression cybernétique, y compris les virus, les vers, les chevaux de Troie, les pirates, les dénis d'exploitation, les systèmes scélérats (rogues), le manque de ressources et l'utilisation abusive tout en proposant les degrés de disponibilité les plus élevés (Industrial Defender, 2008).

Les approches de Verano et de l'*Office of Energy Assurance* sont essentiellement des approches de sécurité informatique visant à se prémunir face à des attaques.

Cependant, la sécurité des systèmes SCADA présente encore certaines problématiques (Krutz, 2006). Les interactions croissantes entre les systèmes de contrôle et les technologies de l'information font que les départements informatiques sont souvent responsables de la sécurité des systèmes de contrôle. Cependant, les responsables informatiques ne sont pas forcément familiers avec la gestion en temps réel des systèmes SCADA. Cela peut se traduire par des lacunes dans la protection des systèmes SCADA.

La protection des systèmes SCADA est également rendue complexe par la facilité d'accès de certains de ses composants qui sont placés sur les équipements des infrastructures essentielles. En effet, de manière générale, les réservoirs, les barrages, les équipements de traitement d'eau, les canalisations, et usines sont assez faciles d'accès.

Un autre élément important est le mauvais état de certaines infrastructures essentielles vieillissantes. Il suffit de penser au niveau dégradé de nombreux réseaux de production d'eau potable qui est directement lié à l'âge de ces infrastructures. Il faudrait donc renforcer physiquement ces réseaux. Il est en effet difficile de contrôler de manière efficace des infrastructures dont l'état ne permet pas véritablement de remplir leurs missions (Krutz, 2006).

De plus, les approches de Verano et de l'*Office of Energy Assurance* ne prennent pas en compte un élément apparaissant important à savoir l'utilisation qui est faite des données nécessaires aux systèmes SCADA et de manière plus générale au bon fonctionnement des infrastructures essentielles. Il semble important dans un contexte de continuité opérationnelle de considérer la sûreté de fonctionnement des infrastructures essentielles prenant en compte la dépendance aux informations et l'utilisation qui en est faîte. Les systèmes SCADA étant opérés par des humains, leur sécurité passe donc à la fois par une évaluation des risques techniques, mais aussi de ceux reliés au facteur humain (Auffrey, 2008).

De manière générale, ce sont des méthodes classiques d'analyse et de gestion des risques qui sont utilisées pour protéger les systèmes de contrôle à distance et de manière plus générale les infrastructures essentielles.

1.3 L'analyse des risques pour les infrastructures essentielles

Les infrastructures essentielles sont actuellement étudiées par le biais d'analyses de risques que nous pouvons qualifier de « classiques ». Ces études ne considèrent généralement que des événements précis (scénarios) pouvant entraîner une défaillance (CAN\CSA, 1997). Elles sont normalement axées sur l'obtention d'un résultat unique (risques économique, technique ou industriel) et se basent sur l'étude d'un nombre fini d'événements naturels ou techniques (Stedinger et coll., 1996 ; Quach et coll., 2000).

De plus, l'analyse des catastrophes passées indique que les méthodes actuelles d'analyse des risques ne reflètent qu'en partie le risque réel de défaillance des réseaux. L'origine des incidents combine des événements naturels à des dysfonctionnements techniques et à des interventions humaines. Les infrastructures essentielles sont non seulement soumises à de nombreux aléas naturels, mais leurs composantes diffèrent également en ce qui concerne leur âge, leur état, leur nature et leur mode de conception. De plus, les modes de gestion utilisés font intervenir à la fois des systèmes automatisés et des manœuvres humaines. Or plusieurs catastrophes sont dues ou amplifiées par des erreurs humaines (Reason, 1993 ; Hubert et Ledoux, 1999).

L'approche classique d'analyse des risques consiste à étudier une infrastructure essentielle à partir d'un nombre fini de causes potentielles de défaillance. Elle ne permet pas de considérer l'ensemble des situations. Au regard de la nature des infrastructures essentielles et des conséquences humaines et socio-économiques qu'entraînent leurs défaillances, il est dangereux de ne pas avoir une image complète des situations possibles.

Une infrastructure essentielle peut-être vulnérable à de nombreux types d'aléas (naturels, humains et techniques). Il est donc nécessaire de tous les considérer dans l'analyse des risques pouvant affecter un réseau. Cependant, actuellement, les différents types d'aléas (naturels, techniques et humains) sont souvent étudiés de manière indépendante.

Les aléas naturels sont essentiellement pris en compte en considérant uniquement des événements exceptionnels. Le problème d'une telle pratique réside dans la faible prévisibilité de ces événements. De ce fait, l'évaluation des aléas naturels est essentiellement effectuée à l'aide de méthodes quantitatives et prédictives basées sur des analyses statistiques et des modélisations stochastiques (Bier et coll., 1999 ; IPCC, 2001 ; Zielinski, 2001).

De plus, l'analyse des aléas naturels généralement basée sur des études historiques, morphologiques et cartographiques présente certaines limites. La première est liée à l'approche considérant un événement unique (scénario). Cette approche est généralement employée pour les études portant sur les aléas naturels. La seconde limite est liée aux besoins des responsables des infrastructures essentielles d'évaluer non seulement le scénario le plus défavorable, mais également l'ensemble des situations auxquelles ils peuvent être confrontés. En effet, les gestionnaires de réseau doivent être en mesure de comprendre le comportement dynamique de leur réseau de façon à prévoir des actions d'atténuation (Robert et coll., 2003b).

Les aléas techniques se rencontrent principalement au niveau de la conception, de la construction, de l'opération et de l'entretien. Ces dysfonctionnements sont liés aux facteurs humains. Il n'est donc pas aisé de différencier les deux, c'est pour cela que la notion de risque sociotechnologique est souvent employée. En effet, même dans le cas d'un bris mécanique, l'action humaine ne peut être écartée en ce sens que ce bris peut être la résultante d'une erreur de conception ou d'un mauvais entretien (Denis, 1998). L'approche théorique habituelle a donc tendance à relier les

causes humaines aux causes technologiques. Une multitude d'outils, plus ou moins spécialisés et dédiés à des activités, telle que la conception, l'opération, l'entretien ou la gestion d'un réseau, existe. Certains modèles, en particulier, permettent de simuler un aléa technologique et de mesurer le comportement du réseau face à cet aléa. Les organisations responsables des infrastructures civiles disposent, en général, de modèles leur permettant de simuler et d'opérer leur réseau d'un point de vue technologique.

Pour analyser les risques technologiques, deux approches d'évaluation existent soit l'approche déterministe, qui est très utilisée en Amérique du Nord, et l'approche probabiliste (Petit, 2003).

L'approche déterministe, qui est basée sur l'utilisation de scénarios sans égard à leur probabilité, correspond à un mode d'analyse et de gestion des risques impliquant des mesures certaines ou traitées comme telles (modèles déterministes, phase déterministe, analyse de sensibilité déterministe). De nombreuses méthodes déterministes existent telles que les arbres (de causes, d'événements, d'utilité), les blocs-diagrammes, Et-si, *Hazard and operability study* (HAZOP), *Failure mode effect and criticity analysis* (FMECA), etc. (Denis, 1998 ; Modarres et coll., 1999 ; Petit, 2003).

L'approche probabiliste correspond à une analyse quantitative de risque et à un mode de gestion des risques impliquant l'évaluation des risques à l'aide de la théorie des probabilités. Le problème d'une telle approche, qui demeure l'approche classique en ingénierie, est qu'elle est basée, comme le souligne Denis (1998), sur le principe que les événements futurs seront similaires à ceux passés et que de toute façon le niveau de sécurité actuel des installations technologiques est tel que le système est protégé face à une succession d'événements autres que ceux observés. De plus, en raison du manque de données relatives aux phénomènes exceptionnels, les résultats obtenus à l'aide de ces méthodes apparaissent fortement subjectifs.

Les méthodes déterministes semblent donc plus adaptées à l'analyse des risques industriels. Toutefois, ces méthodes semblent limitées quant à leur degré de précision. En effet, les résultats obtenus avec de telles méthodes sont difficilement reproductibles. Ceci tient au fait qu'elles font appel à des équipes multidisciplinaires dont la composition peut varier d'une étude à l'autre. De plus, elles ne présentent pas de principes et de critères précis permettant d'encadrer l'analyse ce qui augmente le degré de subjectivité.

Il serait donc nécessaire de définir des critères d'encadrement de l'analyse et de définition des éléments sur lesquels elle devrait porter.

Si les aléas naturels et techniques sont relativement bien connus et intégrés dans les analyses des risques, l'aléa humain, en revanche, est, à bien des égards, minimisé lors de ces études (Petit, 2003). Toutefois, la considération de cet aléa s'avère très importante dans un contexte d'amélioration de la continuité opérationnelle des infrastructures essentielles. En effet, ce sont les humains qui contrôlent les réseaux.

La considération de l'aléa humain dans les analyses de risques est complexe en raison de ses caractéristiques. En effet, il faut différencier la fiabilité humaine de l'erreur humaine (Nicolet et Celier, 1985 ; Petit, 2003). La fiabilité humaine correspond à la réalisation d'une opération dans des limites acceptables. L'erreur humaine, quant à elle, survient lors du dépassement de ces limites. Toutefois, il faut, comme le précise Heidi Ivic (Organisation de Coopération et de Développement économique [OCDE], 2003), considérer l'être humain comme un facteur de sécurité qui dépend de sa formation et de sa motivation. En ce sens, l'aléa humain doit être abordé sous l'angle de la fiabilité humaine et non seulement sous celui de l'erreur humaine.

La complexité de l'aléa humain est également augmentée par le fait qu'il faut à la fois considérer les modèles de l'erreur humaine (Reason, 1993 ; Vanderhaegen, 2003) et les caractères latents et actifs de ces erreurs (Reason, 1993). Toutefois, il

est difficile de prévoir et de quantifier le facteur de risque humain en raison de deux principes fondamentaux.

Le premier est que le fort développement technologique actuel induit nécessairement une augmentation des erreurs humaines (Vanderhaegen, 2003). En effet, les nouveaux équipements évoluent tellement rapidement, en vitesse et en complexité, qu'ils s'accompagnent souvent d'un manque de préparation (entraînement) des utilisateurs. Dans ce contexte, l'ignorance potentielle concernant les pratiques à mettre en œuvre en cas de défaillance de nouveaux systèmes est un facteur d'aggravation du risque.

Le deuxième est que les erreurs humaines sont des phénomènes quotidiens et que, dans la majorité des cas, leurs impacts sont négligeables. Il apparaît alors impossible de les éviter d'autant plus que les facteurs humains, induisant ces erreurs, ne peuvent pas être supprimés.

Les méthodes portant sur l'aléa humain sont très nombreuses (Petit, 2003). Elles peuvent être regroupées suivant des classifications différentes. Nous présenterons ici celle de Keravel (1997) qui se base sur les différentes phases de développement des méthodes :

- phase 1 de 1966 à 1974

  Cette première phase correspond à l'utilisation de méthodes d'analyse de dysfonctionnement technique, telles que les arbres de défaillance, *Hazard and operability study* (HAZOP) et l'Analyse des modes de défaillance, de leurs effets et de la criticité (AMDEC). Ces méthodes de dimension technique ne permettent pas véritablement de prendre en compte les facteurs humains.
- phase 2 de 1980 à 1983

  Cette deuxième phase correspond au développement de méthodes d'estimation par jugements d'experts et évaluation calculée, telle que la *Tecnica empirica stima errori operatori* (TESEO) et la *Technique for human error rate*

prediction (THERP). Ces méthodes intègrent véritablement la composante humaine, mais vont négliger la structure d'analyse.

- phase 3 de 1984 à 1987
  Cette troisième phase correspond au développement de méthodes, telles que la *Systematic human error reduction and prediction approach* (SHERPA) et de la *Human error assessment and reduction technique* (HEART), qui précisent mieux la composante humaine et qui prennent en considération les facteurs qui l'influencent.
- phase 4 à partir de 1988
  Cette quatrième phase correspond au développement de méthodes, telles que la Méthode d'évaluation de la réalisation des missions opérateur pour la sûreté (MERMOS), qui visent à prendre en compte de façon simultanée les facteurs humains et techniques.

Les méthodes d'analyse de l'aléa humain évoluent donc vers une prise en compte des différents facteurs, tant externes qu'internes, qui vont influencer l'homme. Cette évolution conduit à développer des méthodes de plus en plus complexes et relativement lourdes à mettre en œuvre. En pratique, ce sont encore les méthodes, correspondant à la première phase de développement, qui sont le plus utilisées en raison de leur relative simplicité de mise en œuvre.

Il n'est pas, à mon avis, utile d'utiliser des méthodes de la phase 4 avec un tel niveau de développement. En effet, il faut étudier un réseau de façon systémique et en ce sens, AMDEC et HAZOP peuvent très bien convenir à condition d'intégrer de façon plus importante le facteur humain et de permettre la mise en œuvre d'une phase de prévention des risques. De plus, ces méthodes ont comme avantages indéniables d'être relativement faciles et rapides à utiliser tout en permettant de visualiser le réseau étudié dans son ensemble.

Toutefois, aucune méthode n'est véritablement meilleure qu'une autre. Quelle que soit la méthode employée, il est important de garder à l'esprit que les résultats obtenus ne constituent pas forcément les seuls possibles.

L'approche classique d'analyse de risques, consistant à étudier un système à partir d'un nombre fini de causes potentielles de défaillance, ne permet donc pas de considérer l'ensemble des aléas (naturels, techniques et humains). Il est en effet assez complexe de combiner des méthodes d'analyses considérant des aléas de natures différentes. De ce fait, les facteurs humains et organisationnels sont le plus souvent minimisés. Graham Creedy spécifie même que les analystes ne s'interrogent que très rarement sur les motivations des décideurs qui peuvent être génératrices de vulnérabilités (OCDE, 2003).

Nous venons de voir l'approche classique prédominant en sécurité industrielle. Toutefois, nous n'avons pas encore vu les méthodes spécifiques au risque informatique. Ces méthodes sont importantes à étudier, car elles sont utilisées pour les systèmes informatiques qui sont à la base des systèmes SCADA.

1.4 Le risque informatique

Le risque informatique est très complexe de par le fait qu'il regroupe de nombreux domaines différents, tels que la programmation, le développement de logiciel, la sécurité des réseaux, etc. Cette complexité est amplifiée par le développement des nouveaux moyens de communication, tels qu'Internet, qui nécessite la mise en place de nouveaux moyens de contrôle.

Nous n'aborderons pas ici tous les aspects concernant les problèmes de copyright et de droits d'auteurs de même que les techniques développées pour se prémunir face à la cybercriminalité (antivirus, coupes-feu, filtres, etc.).

Nous nous concentrerons sur les moyens de prévention et les méthodes d'analyse des risques permettant de renforcer la sécurité des entreprises face aux problèmes

informatiques. Pour une entreprise donnée, la considération du risque informatique est d'autant plus complexe qu'elle ne se limite pas au seul cadre informatique. En effet, il est également nécessaire de considérer des facteurs organisationnels, des problèmes de sécurisation des bâtiments, etc.

Il peut donc s'avérer difficile d'analyser les vulnérabilités d'un réseau informatique. Pour se faire, de nombreuses méthodes de sécurisation ont été développées. Nous pouvons citer par exemple les méthodes Intégration dans la conception des applications de la sécurité (INCAS), Méthode d'administration et de gestion des droits et accréditations (MAGDA), Méthodologie d'analyse de risques informatiques orientée par niveaux (MARION) ou Méthode harmonisée d'analyse de risques (MEHARI) (CLUb de la Sécurité des systèmes d'Information Français [CLUSIF], 1997 ; CLUSIF, 1999 ; CLUSIF, 2003 ; Stampf, 2002). Grâce à ces méthodes, les Responsables de la sécurité des systèmes d'information (RSSI) peuvent élaborer des plans de sécurité.

Nous ne présenterons que la méthode MEHARI qui a été développée par le CLUSIF. Ce choix est dicté par le fait que cette méthode est récente et qu'elle intègre les principes à la base des autres méthodes. De plus, la méthode MEHARI est actuellement employée pour certaines infrastructures essentielles.

MEHARI est une méthode d'analyse des risques, élaborée à partir des méthodes MARION et MELISA, qui fonctionne sur des principes similaires à ceux de la méthode INCAS.

Le but de MEHARI est de mettre à disposition des règles, des modes de présentation et des schémas de décision de façon à proposer (CLUSIF, 2003) :

- des Plans stratégiques de sécurité (PSS) visant à fixer les objectifs de sécurité et définir la politique de sécurité ;
- des Plans opérationnels de sécurité (POS) visant à planifier les actions de sécurité à partir d'audit et d'évaluation de gravité des scénarios choisis ;

- des Plans opérationnels d'entreprise (POE) visant à définir des scénarios et élaborer des indicateurs pour définir un niveau de gravité des risques potentiels.

Ces plans se traduisent par un ensemble cohérent de mesures permettant de palier les failles constatées et d'atteindre le niveau de sécurité répondant aux exigences des objectifs fixés.

Pour développer ces plans, MEHARI considère trois facteurs caractérisant la potentialité du risque (exposition naturelle, intention de l'agresseur et possibilité de sinistre) ainsi que trois caractérisant son impact (détériorations, dysfonctionnements, pertes finales).

La potentialité du risque intègre trois facteurs :

- accidents ;
- erreurs ;
- malveillances.

Les impacts intègrent également trois facteurs de sécurité :

- disponibilité ;
- intégrité ;
- confidentialité.

La considération de la potentialité de risque et des impacts permet de spécifier la gravité du risque qui varie de 0 à 4 :

- la cotation 0 correspond à une gravité du risque faible ;
- la cotation 1 correspond à une gravité du risque acceptable ;
- la cotation 2 correspond à une gravité du risque tolérée ;
- la cotation 3 correspond à une gravité du risque inadmissible ;
- la cotation 4 correspond à une gravité du risque inacceptable.

Une fois les facteurs de risque analysés, MEHARI définit différentes mesures de sécurité pour réduire la gravité du risque. Il existe six types de mesures de sécurité, chacun agissant sur un des facteurs de risque :

- mesures structurelles pour l'exposition naturelle ;
- mesures dissuasives pour l'intention de l'agresseur ;
- mesures préventives pour la possibilité de sinistre ;
- mesures de protection pour la gravité des détériorations ;
- mesures palliatives pour la gravité des dysfonctions ;
- mesures de récupération pour la gravité des pertes finales.

MEHARI est plus qu'une méthode d'analyse des risques. En effet, c'est un regroupement d'outils de gestion des risques informatiques et plus particulièrement des problèmes de sécurité. Toutefois, MEHARI présente encore le problème de l'approche par scénario.

Les méthodes d'analyse de risque informatique sont essentiellement basées sur des audits et des approches d'analyse de risque par scénarios ce qui limite leur portée. Elles ne visent pas à définir des probabilités, mais des potentialités d'événements ce qui s'avère intéressant. Toutefois, elles semblent limitées quant à la considération de la fiabilité humaine. Elles se concentrent plus sur les composantes techniques des systèmes informatiques de façon à accroître la sécurité des accès aux ressources informatiques.

Ces méthodes sont sans doute très pertinentes pour le renforcement des systèmes informatiques bien qu'elles puissent être relativement lourdes à mettre en œuvre. Toutefois, elles ne permettent pas une approche d'analyse de risque globale qui considèrerait à la fois les composantes humaines et techniques des systèmes informatiques et celles des autres systèmes constitutifs d'une infrastructure essentielle.

Pour avoir une approche globale, il faudrait, dans un premier temps, considérer l'infrastructure essentielle étudiée et son réseau informatique comme étant indépendants. Les deux réseaux pourraient être étudiés chacun de leur côté. L'analyse de risque du réseau informatique pourrait utiliser des méthodes de sécurisation informatique comme MEHARI. L'analyse de risque de l'infrastructure essentielle pourrait employer les méthodes développées pour la sécurité industrielle. Dans un deuxième temps, il s'agirait de considérer les vulnérabilités du réseau informatique comme étant des générateurs de risque et donc des aléas exogènes pour l'infrastructure essentielle.

Cette approche permettrait de véritablement considérer l'ensemble des aléas pouvant affecter une infrastructure essentielle. Le fait de considérer le réseau informatique comme étant une structure indépendante s'explique aussi par l'organisation des infrastructures essentielles. En effet, habituellement, le service informatique constitue une division indépendante au sein d'une entreprise.

Cependant, il apparaît encore plus important dans un contexte d'amélioration de la résilience des infrastructures essentielles de considérer la dépendance de ces infrastructures face aux données cybernétiques. Il est possible de cette manière d'améliorer la continuité opérationnelle des infrastructures essentielles en considérant les données comme une ressource particulière. L'utilisation des méthodes de sécurité informatique sert alors à améliorer la qualité de transfert de cette ressource.

En regard de la nature même des infrastructures essentielles avec les conséquences humaines et socio-économiques qu'elles entraînent lors de leurs défaillances, il est dangereux de ne pas avoir une image complète des situations possibles. Les méthodes d'analyse des risques et des vulnérabilités des infrastructures essentielles doivent donc prendre en compte la cybernétique et la fiabilité humaine. La protection des infrastructures essentielles ne doit pas se limiter à une analyse des risques. Elle doit être intégrée dans un processus global de gestion des risques.

1.5 Conclusion

La revue de littérature effectuée fait ressortir plusieurs éléments particulièrement importants qui sont à la base de ce travail de recherche.

Le premier est que le domaine des mesures d'urgence est en pleine effervescence actuellement. Ce domaine qui était traditionnellement sous la responsabilité des militaires est passé, petit à petit, vers la fin du XXe siècle sous celle de la société civile. Cela a entraîné une modification des législations et dans certains cas des façons de faire. En raison des attentats du 11 septembre 2001 aux États-Unis, la tendance tend à se modifier à nouveau avec de plus en plus de préoccupations portant sur les moyens de se préparer et de se protéger face au terrorisme.

Le deuxième élément important est, dans ce contexte de redéfinition de la gestion des risques et des mesures d'urgence, l'importance de plus en plus grande que prennent les recherches concernant les infrastructures essentielles, leurs interdépendances et les relations de dépendance de la société face à ces réseaux qui sont le plus souvent privés. Il s'agit donc de gérer les risques inhérents à l'utilisation de méga-infrastructures tout en intégrant la problématique de la confidentialité des données reliées à leur gestion pour des raisons de sécurité.

Cette constatation nous amène à un troisième élément important portant sur le mode de gestion des infrastructures essentielles. Ces méga-structures sont de plus en plus informatisées et de par le fait même dépendantes des grandes quantités de données nécessaires à leur bon fonctionnement. De nombreuses méthodes de gestion des risques informatiques existent. Elles sont certainement adaptables pour les infrastructures essentielles. Cependant, elles ne considèrent que peu le facteur humain qui est prépondérant dans un contexte de gestion et de continuité opérationnelle. De plus, elles se focalisent sur l'outil informatique et non, à notre avis, sur l'élément le plus important, l'information. L'information est le nerf de la guerre. Il faut donc intégrer la considération de la cybernétique dans l'analyse des infrastructures essentielles. Il est donc important d'intégrer dans les méthodes

d'analyse de risques et de vulnérabilité, la prise en compte du contrôle des infrastructures essentielles par l'entremise des systèmes SCADA. La majorité des méthodes d'analyse de risque existantes considère la cybernétique sous l'angle de la sécurité des infrastructures essentielles face à des cybermenaces (virus, vers, chevaux de Troie, etc.).

Il paraît important d'analyser la gestion des risques pour les infrastructures essentielles d'un point de vue global en intégrant la composante cybernétique comme une ressource de manière à améliorer les processus de continuité opérationnelle. Il faut pour cela, aborder la problématique de la dépendance aux données des infrastructures essentielles en considérant ces données comme des ressources essentielles. Cette considération des données doit être abordée en considérant la sûreté et la qualité de fonctionnement des infrastructures essentielles, c'est-à-dire en analysant les vulnérabilités des infrastructures essentielles par rapport à l'utilisation des données et l'effet de la dégradation de ces données sur la continuité opérationnelle des infrastructures essentielles. En effet, la problématique de la cybernétique n'est pas uniquement une problématique de sécurité informatique et de protection des systèmes automatisés. Il faut également considérer l'utilisation qui est faite de l'information et comment une dégradation de cette information ou de son transfert peut affecter une infrastructure essentielle et la réalisation de sa ou ses missions.

Cette thèse se propose donc de définir la différence entre risque et vulnérabilité, de proposer une méthodologie d'analyse des vulnérabilités adaptée aux infrastructures essentielles et finalement de proposer un mode de prise en compte de la problématique cybernétique dans cette méthodologie.

Le chapitre suivant présente les hypothèses et les objectifs qui sous-tendent ce travail de recherche.

CHAPITRE 2 PROBLÉMATIQUE, HYPOTHÈSES ET OBJECTIFS

2.1 Problématique et objectif principal de ce travail

La gestion des risques portant sur les systèmes complexes, telle que les infrastructures essentielles, est en plein développement depuis le début du XXIe siècle. Les méthodes d'analyse de risque développées pour gérer le risque se réfèrent de plus en plus à la notion de vulnérabilité sans qu'il soit pour autant facile de la différencier du concept de risque.

Il paraît donc important de définir exactement à quoi correspondent le risque et la vulnérabilité associés à un système complexe. Une fois ces concepts établis, il sera en effet plus facile de poser les bases d'une véritable méthodologie d'analyse de vulnérabilité.

De plus, la majorité des approches de gestion des risques portant sur les infrastructures essentielles favorise des études à grande échelle intégrant les réseaux dans leur ensemble. Cela pose deux problèmes majeurs :

- la difficulté d'utiliser une approche inductive de gestion des risques de par le fait de l'impossibilité d'appréhender l'ensemble des aléas pouvant affecter une infrastructure essentielle dans sa globalité ;
- la difficulté de considérer les particularités régionales de certaines parties de l'infrastructure essentielle. En effet, une infrastructure essentielle peut comporter des missions particulières pour des secteurs géographiques précis.

Il est également difficile de prendre en compte, dans les analyses de risque actuelles, la dépendance d'un système relativement à l'utilisation de l'outil cybernétique et plus spécifiquement des données. Cet élément est particulièrement important pour les infrastructures essentielles qui sont de plus en plus contrôlées à distance par l'entremise de systèmes SCADA. Cependant, la majorité des études intégrant cette problématique le font du point de vue de la sécurité par la considération des attaques malveillantes des systèmes. Il paraît important de

considérer aussi l'effet de la perte ou de la dégradation de données qui peuvent également survenir en situation normale.

Dans ce contexte, le but de ce projet de doctorat est de ***proposer les principes méthodologiques qui permettront d'évaluer la vulnérabilité d'une infrastructure essentielle reliée à l'utilisation de données cybernétiques***. Il ne s'agit pas d'étudier les systèmes en matière de sécurité, ce qui relève plus du Génie informatique ou du Génie logiciel, mais bien de les analyser en termes de sûreté de fonctionnement. Ce projet s'inscrit dans une démarche globale visant à évaluer de façon systémique et systématique les dépendances et interdépendances pouvant affecter les infrastructures essentielles. Le gestionnaire aura alors une connaissance accrue des transferts de vulnérabilités tant internes qu'externes pouvant affecter son réseau. De plus, l'intégration de cette recherche dans les études de risque permettra d'établir les principes méthodologiques permettant de renforcer la continuité opérationnelle et les mesures d'urgence établies de même que les mécanismes opérationnels de communication du risque. Cela contribuera ainsi à une amélioration de la protection des personnes et des biens.

Pour atteindre le but de ce projet, nous posons plusieurs hypothèses de travail qui sont présentées dans la section suivante.

2.2 Hypothèses

De manière concrète, cette recherche se base sur quatre hypothèses de travail :

Hyp. 1. Le concept de vulnérabilité et la notion d'état d'un système sont des composantes intrinsèques du risque ;

Pour vérifier cette hypothèse, nous analyserons les définitions existantes du risque et de vulnérabilité. Nous montrerons l'utilité de considérer la variation de l'état du système analysé et comment ce concept doit être intégré dans la définition et surtout l'analyse du risque.

Hyp. 2. Une infrastructure essentielle peut être définie en fonction de ses missions, fonctions et besoins (ressources essentielles) ;

Pour vérifier cette hypothèse, nous caractériserons la structure organisationnelle d'une infrastructure essentielle. Nous vérifierons si une structure générale (missions, fonctions, ressources) peut s'appliquer quelle que soit l'infrastructure essentielle considérée.

Hyp. 3. L'analyse de la vulnérabilité d'une infrastructure essentielle peut se faire de manière déductive en partant des conséquences de défaillances et en remontant vers les ressources essentielles, se poser la question « Pourquoi/Comment » plutôt que « Et-Si/Comment » ;

Pour vérifier cette hypothèse, nous présenterons les principes permettant d'effectuer une analyse de risques déductive centrée sur la caractérisation d'une infrastructure essentielle. Pour cela, nous proposons d'employer une méthodologie recentrée sur un niveau de conséquences acceptables.

Hyp. 4. Le risque cybernétique peut être analysé en considérant les données comme des ressources essentielles d'une infrastructure essentielle ;

Pour vérifier cette hypothèse, nous présenterons les particularités des données cybernétiques et comment il est possible de considérer la dépendance d'une infrastructure essentielle face à ce type de ressource.

La vérification des hypothèses, posées comme prémisses à cette recherche, permettra de juger de la réussite des travaux qui seront effectués. En effet, bien que le but ultime de ce projet de doctorat soit de proposer des principes méthodologiques d'évaluation des vulnérabilités opérationnelles d'une infrastructure essentielle, ce travail devra également permettre de confirmer ou

d'infirmer les hypothèses de départ. Pour ce faire, cette recherche visera à atteindre des objectifs spécifiques.

2.3 Objectifs spécifiques

De manière concrète, la vérification de nos hypothèses de travail nécessite l'atteinte de cinq (5) objectifs spécifiques :

Objectif 1. **Définir** les concepts de risque et de vulnérabilité ;
Cet objectif permettra de vérifier la première hypothèse.

Objectif 2. **Caractériser** les différents groupes de fonctions constitutives d'une infrastructure essentielle ;
Cet objectif permettra de vérifier la deuxième hypothèse.

Objectif 3. **Caractériser** les besoins essentiels d'une infrastructure essentielle ;
Cet objectif permettra de vérifier la deuxième et la troisième hypothèse.

Objectif 4. **Définir** les principes d'une méthode systémique et systématique d'analyse de vulnérabilité d'une infrastructure essentielle ;
Cet objectif permettra de vérifier la troisième hypothèse.

Objectif 5. **Définir** et **caractériser** comment intégrer la cybernétique dans la méthode développée ;
Cet objectif permettra de vérifier la quatrième hypothèse.

En nous focalisant sur ces objectifs de définitions et de caractérisations de concepts, nous vérifierons nos hypothèses, à tout le moins d'un point de vue théorique, en mettant l'emphase sur la manière dont les concepts proposés s'articulent entre eux. En ce qui concerne la vérification pratique de nos

hypothèses, nous présenterons certains travaux qui ont été amorcés ou réalisés à partir des concepts que nous développerons.

Pour vérifier les hypothèses et favoriser l'atteinte de nos objectifs spécifiques, la méthodologie de recherche proposée est constituée de différents volets correspondant à ces objectifs spécifiques. En procédant de cette façon, les hypothèses pourront être vérifiées en cours de recherche.

2.4 Type de recherche

Cette recherche a deux orientations :

- la première, qui est fondamentale, vise à définir ou à préciser des principes, des concepts ;
- la deuxième, qui est appliquée, correspond à une étude de faisabilité. Elle vise à montrer la possibilité de développer une méthodologie d'étude de vulnérabilité des infrastructures essentielles qui prend en compte les dépendances aux données cybernétiques.

De manière concrète, cette recherche débute par une revue de littérature de façon à connaître l'état actuel de la connaissance dans le domaine de la gestion des risques appliquée aux infrastructures essentielles. C'est d'ailleurs cette revue de littérature qui a permis de préciser la problématique présentée dans ce chapitre.

Cet état de la connaissance sera complété par une étude à la fois empirique, pour ce qui est de la détermination des différents types d'opérations d'une infrastructure essentielle, et descriptive, pour l'intégration des données cybernétiques dans le fonctionnement des infrastructures essentielles.

Par la suite, la recherche consistera en une phase de développement d'une méthode systématique et systémique d'évaluation des vulnérabilités.

2.5 Organisation de la thèse

Ce travail est organisé en six chapitres :

- Le premier chapitre est une revue de littérature qui présente l'avancement des travaux dans le domaine de la gestion des risques associés aux infrastructures essentielles, mais aussi un état des méthodes d'analyse de risques développées dans le cadre des risques informatiques ;
- Le deuxième chapitre présente la problématique que veut aborder ce travail de même que les hypothèses et les objectifs fixés pour la résoudre ;
- Le troisième chapitre définit le concept de risque de même que ceux de vulnérabilité et de résilience qui sont basés sur l'état du système étudié ;
- Le quatrième chapitre aborde l'organisation des infrastructures essentielles et la manière dont elle devrait être caractérisée pour être intégrée dans une méthode d'analyse de risques ;
- Le cinquième chapitre présente les principes de la méthodologie que nous proposons pour analyser le risque. Cette méthodologie est adaptée à notre définition du risque et intègre les caractéristiques propres aux infrastructures essentielles. Ce chapitre présente également les particularités liées aux données cybernétiques et la manière de les intégrer dans la méthodologie d'analyse de risques que nous proposons ;
- Le sixième chapitre présente une discussion sur la vérification des hypothèses de ce travail de recherche. Il aborde également de manière plus générale quelques réflexions sur la méthodologie proposée.

Le Tableau 2.1 présente les chapitres ainsi que les hypothèses et objectifs qu'ils permettront d'aborder.

Maintenant, que l'organisation de ce travail est établie, nous allons aborder dans le prochain chapitre la notion de risque. Nous définirons ce concept de risque, mais également ceux de vulnérabilité et de résilience. Nous verrons également comment ces trois notions s'intègrent entre elles.

Tableau 2.1 - Organisation de la thèse.

Chapitre	Hypothèse et objectifs abordés
1 : Revue de littérature	
2 : Problématique	
3 : Concept de risque	**Hyp. 1 :** Le concept de vulnérabilité et la notion d'état d'un système sont des composantes intrinsèques du risque. **Obj. 1 : Définir** les concepts de risque et de vulnérabilité.
4 : Caractérisation d'une infrastructure essentielle	**Hyp. 2 :** Une infrastructure essentielle peut être définie en fonction de ses missions, fonctions et besoins (ressources essentielles). **Obj. 2 : Caractériser** les différents groupes de fonctions constitutives d'une infrastructure essentielle. **Obj. 3 : Caractériser** les besoins essentiels d'une infrastructure essentielle.
5 : Méthodologie d'analyse de risque	**Hyp. 3 :** L'analyse de la vulnérabilité d'une infrastructure essentielle peut se faire de manière déductive en partant des conséquences de défaillances et en remontant vers les ressources essentielles, se poser la question « Pourquoi/Comment » plutôt que « Et-Si/Comment ». **Obj. 4 : Définir** les principes d'une méthode systémique et systématique d'analyse de vulnérabilité d'une infrastructure essentielle. **Hyp. 4 :** Le risque cybernétique peut être analysé en considérant les données comme des ressources essentielles d'une infrastructure essentielle. **Obj. 5 : Définir** et **caractériser** comment intégrer la cybernétique dans la méthode développée.
6 : Discussion et vérification des hypothèses de recherche	Toutes les hypothèses et tous les objectifs de recherche seront abordés dans ce chapitre

CHAPITRE 3 CONCEPTS DE VULNÉRABILITÉ, DE RISQUE ET DE RÉSILIENCE

Le concept de vulnérabilité est extrêmement important dans un contexte de gestion des risques et plus particulièrement en ce qui a trait aux infrastructures essentielles. En effet, comme nous l'avons vu lors de la revue de littérature, la majorité des travaux abordant la problématique de la sécurité des infrastructures essentielles font référence au concept de vulnérabilité. Cependant, ce concept se confond parfois avec celui de risque. La notion de résilience est également de plus en plus utilisée tout en sachant difficilement à quoi fait référence ce concept. Il apparaît donc important de clarifier ces concepts de risque, de vulnérabilité et de résilience de même que de poser les définitions qu'auront ces termes dans le cadre de ce travail. C'est ce que se propose de faire ce chapitre.

3.1 Les risques, les vulnérabilités et la résilience

Les domaines de la sécurité civile et de la continuité opérationnelle s'articulent autour de la gestion des risques. Le concept de risque est en lui-même complexe. Il existe presque autant de définitions du risque que de domaine d'application. Le risque ne sera pas perçu de la même façon dans le domaine de la santé que dans celui de la finance (Bernard et coll., 2002). Cependant, comme le montre Seidou (2002), les définitions, bien que nombreuses, se basent presque toutes sur la nature du risque et essayent d'en donner une valeur chiffrée. Le risque est alors défini comme un produit ou une fonction de deux éléments (une probabilité et une conséquence ; un aléa et un enjeu). Depuis les années 50, les scientifiques ont une approche probabiliste du risque en le définissant comme une « espérance mathématique » de dommages possibles (CNFSH, 2003). Toutefois, d'autres approches, telles que celle de Kaplan (1997), définissent le risque comme la combinaison d'un triplet d'information caractéristique du risque (événement causant le risque, probabilité et sévérité du risque ; scénarios, conséquences négatives, vraisemblance du couple scénario-conséquence). Toutefois, ces nombreuses définitions du risque ne s'opposent pas. Fondamentalement, le risque est une

combinaison de deux facteurs. C'est la combinaison de la possibilité d'apparition d'un aléa et de ses conséquences sur des enjeux.

Traditionnellement, la sécurité industrielle de même que le domaine des catastrophes naturelles abordent la problématique des risques majeurs. Le risque est alors défini, de manière classique, comme la combinaison de la probabilité d'un aléa pouvant affecter un système et des conséquences que cela peut engendrer au niveau du système et de son environnement direct. La différence principale est que sont considérés uniquement les scénarios engendrant des conséquences importantes (catastrophes). La méthodologie d'analyse des risques du Conseil pour la réduction des risques industriels majeurs (CRAIM) est un parfait exemple de cette approche par scénarios (Figure 3.1).

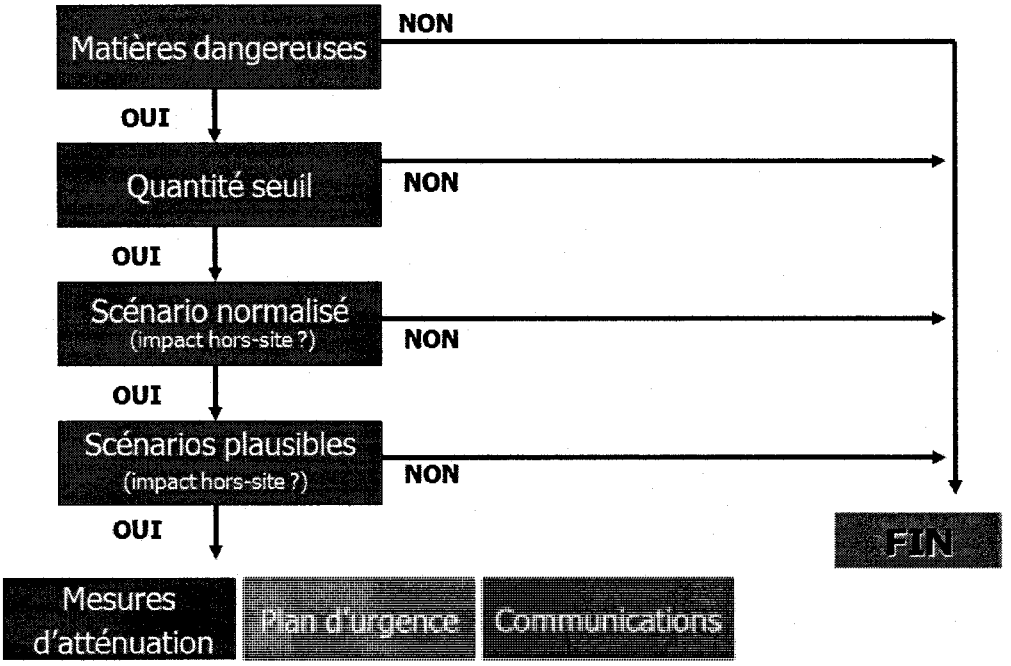

Figure 3.1 - Processus d'analyse des risques (CRAIM, 2007).

Cette approche est développée pour les industries qui utilisent et entreposent des produits chimiques. Il s'agit tout d'abord de définir si des matières dangereuses

sont présentes sur le site d'étude dans une quantité supérieure à une quantité seuil. Les matières dangereuses de même que les quantités seuil qui leur sont associées sont définies dans des listes de contrôle fournies, entre autres, par le CRAIM.

Par la suite, si des matières dangereuses se trouvent sur le site dans une quantité supérieure à la quantité seuil, il faut alors calculer des scénarios normalisés, un pour chaque matière dangereuse. Ces scénarios correspondent au *worst case scenarios*. Ils visent à définir un rayon d'impact relié aux effets toxiques et aux explosions ou incendies pouvant être générés par une défaillance impliquant une matière dangereuse donnée. En fait, un scénario normalisé d'accident correspond à la plus grande quantité d'une substance dangereuse, détenue dans le plus gros contenant, dont la distance d'impact est la plus grande en tenant compte uniquement de mesures de protection passive (CRAIM, 2007). Ces scénarios permettent donc de servir de comparaison entre différents systèmes, car ils sont définis et calculés sans intégrer les particularités d'un site donné.

Dans le cas où le rayon d'impact d'un scénario normalisé dépasse les limites de propriété du site où est faite l'analyse des risques, il faut calculer des scénarios alternatifs. Ces scénarios sont plus représentatifs de la réalité. Un scénario alternatif représente un autre type d'accident pouvant se produire. Ce type de scénarios tient compte de la proximité ou de l'interconnexion des contenants de la substance concernée et des mesures de protection passive et active mises en place (CRAIM, 2007).

Une fois que ces deux types de scénarios ont été calculés, il est possible de développer des plans de mesures d'urgence de même que des processus de communication adaptés à la situation.

Nous avons montré un exemple de l'utilisation des scénarios dans le domaine de l'industrie chimique. Ces approches par scénario sont également utilisées dans d'autres domaines. Il est notamment possible de mentionner le cas du modèle

d'Évaluation consolidée des risques (ÉCR) du Programme technique de sécurité publique (PTSP) de Recherche et développement pour la défense Canada (RDDC). Le modèle d'ÉCR proposé débute en effet par le choix d'un scénario de menace ou d'un descripteur de risque. Par la suite, une valeur numérique est attribuée à la faisabilité technique de la réalisation du scénario et à la gravité des conséquences du scénario (RDDC, 2009). Finalement, la vulnérabilité de la mission est déterminée en utilisant une matrice de risques à deux dimensions.

L'utilisation de représentation matricielle pour évaluer le risque est relativement classique. La Figure 3.2 présente un exemple d'une telle matrice.

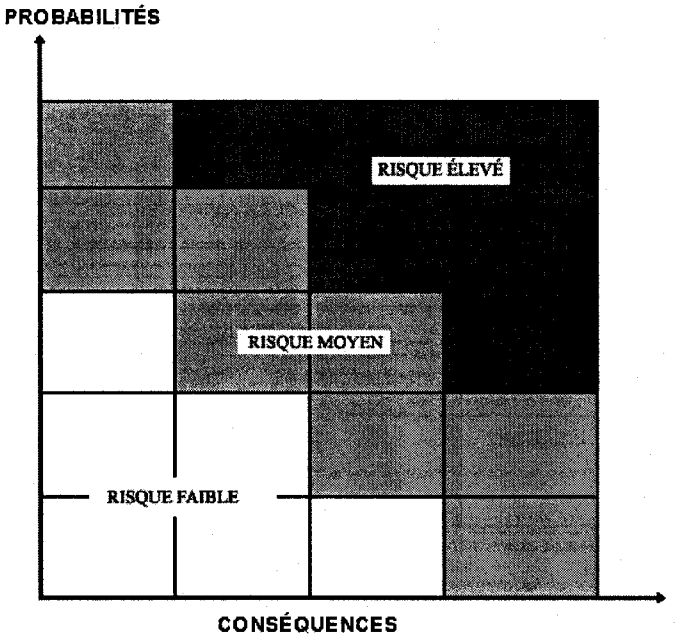

Figure 3.2 - Représentation matricielle du risque.

Dans ce contexte, l'analyse et l'évaluation des risques portent alors sur la zone des aléas à probabilités moyennes et à conséquences moyennes (risque moyen). En effet, il est possible de penser que les risques faibles sont les risques auxquels la population est confrontée régulièrement et en ce sens, il n'est pas forcément nécessaire de les analyser et de les évaluer plus précisément. Nous sommes

habitués à les gérer. Il en est de même pour la partie des risques élevés qui correspondent à des aléas ayant des probabilités d'apparition fortes et des conséquences importantes. Il est possible de penser, comme le précise M. Jacobson, que si de tels risques existaient, l'humanité ne se serait jamais développée (Jacobson, 2004).

Cette représentation du risque pose toutefois quatre problèmes principaux :

- une représentation statique ;
- la non-considération du système ;
- la notion d'acceptabilité du risque ;
- l'incertitude du risque.

Cette représentation est statique dans le sens où elle ne prend pas en compte l'évolution temporelle du risque. En effet, cette représentation est principalement utilisée pour représenter le risque résiduel. Dans la majorité des cas, ce risque est considéré comme le seul risque possible. Il n'y a aucune intégration de la variabilité temporelle de l'ensemble des composantes constituant ce risque.

Le deuxième élément problématique est qu'elle ne considère en aucune façon le système sur lequel agit l'aléa. En fait, elle le prend en compte de manière indirecte par l'entremise des conséquences. Cette manière de procéder est bien adaptée pour les risques majeurs lorsque le pire scénario possible (*worst case scenario*) est considéré. En effet, dans ce cas, l'analyse considère la défaillance totale du système. Par contre, cela ne permet en aucun cas, d'analyser les événements intermédiaires, le mode de réaction du système à ces événements et la gradation des conséquences en découlant.

Le troisième problème tient au fait que la représentation matricielle du risque peut également servir à caractériser l'acceptabilité d'un risque. De manière générale, le risque élevé est considéré comme inacceptable tandis qu'un risque faible est associé à un risque négligeable donc très acceptable. Le risque moyen, quant à lui, est

considéré également comme acceptable si des avantages compensatoires sont présents. C'est le principe du système *As Low As is Reasonably Practical* (ALARP) qui a été développé en Angleterre dans le contexte du cadre d'établissement des critères relatifs aux risques (SNC-Lavalin, 2006). Si, à première vue, le fait de déterminer l'acceptabilité du risque en se basant sur ce type de matrice n'est pas problématique. Cela peut être discuté si les informations contenues dans ce type de matrice sont utilisées seules. En effet, un risque faible donc considéré comme étant négligeable peut engendrer des conséquences importantes.

Prenons l'exemple, du projet Rabaska qui est un projet de port méthanier devant être développé dans la province de Québec.

D'après la Figure 3.3 tirée de l'étude d'impacts sur l'environnement réalisée pour ce projet, les collisions à quai avec fuite d'un méthanier constituent un risque négligeable. En effet, d'après l'étude, le risque d'une collision à quai conduisant à un déversement suivi d'un feu de nuage et causant des décès est négligeable, en raison d'une fréquence d'occurrence de un tous les 9 millions d'années.

Dans ce cas précis, un poids plus important semble donc être mis sur la probabilité d'occurrence de l'aléa plutôt que sur les conséquences pouvant être engendrées.

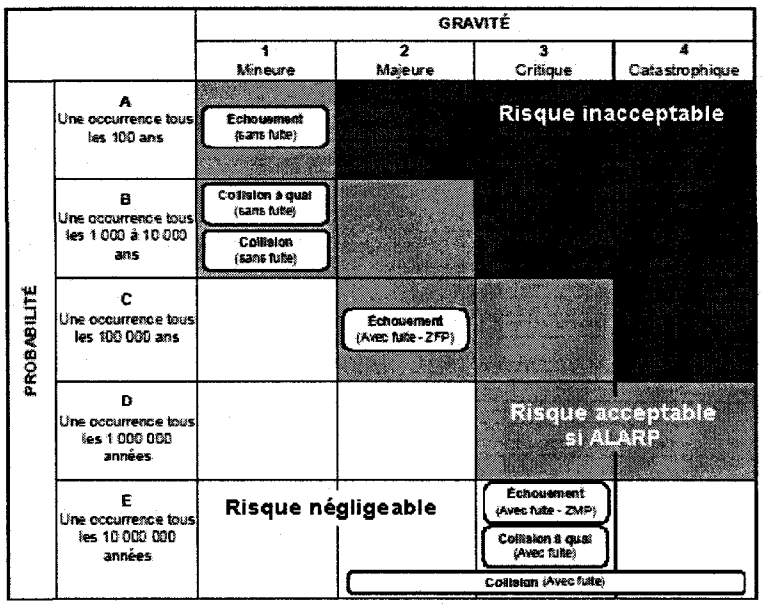

Figure 3.3 - Analyse des risques maritimes pour le projet Rabaska (SNC-Lavalin, 2006).

Il est possible de se questionner sur le fait que ce risque soit ou non négligeable. En effet, les conséquences éventuelles comportent la mort de personnes ce qui, à notre avis, est difficilement acceptable surtout dans le cas d'implantation d'un projet en zone péri-urbaine. De plus, il est possible de s'interroger sur la validité de la détermination de l'occurrence d'un tel événement. L'utilisation d'une matrice de risque pour définir son acceptabilité s'avère être un outil d'aide à la décision très utile, mais il ne se suffit pas à lui-même.

Finalement, le domaine des risques est un domaine où l'incertitude domine. Il peut être dangereux de mettre beaucoup d'emphase sur des probabilités d'apparition d'un aléa donné. En effet, il n'est vraiment pas assuré que le passé soit garant du présent, ni du futur. Cela demanderait une étude statistique poussée, mais surtout qu'aucune modification du contexte d'étude ne survienne. Or, actuellement ce n'est pas forcément le cas. Les événements naturels extrêmes sont souvent considérés comme des « *Act of God* » ce qui traduit leur imprévisibilité. Il est étonnant de vouloir prévoir l'imprévisible. De plus, l'humain agit sur son environnement. Les

événements naturels extrêmes ont tendance à se transformer et à s'accélérer pour devenir des « *Human act* ». Il n'y a qu'à penser aux changements climatiques pour s'en persuader. Ce constat semble aussi valable pour les risques technologiques. Aucun système de même que son environnement ne sont statiques (Johnson et coll., 2007). Ils évoluent et par le fait même les risques qu'ils pourraient induire évoluent également. Ceci est particulièrement vrai si nous pensons aux défaillances en cascade ou effets domino. Il semble donc que les deux seules notions d'aléas et de conséquences ne soient pas suffisantes pour qualifier le risque et particulièrement l'évolution du système et de son environnement.

Pour palier ce problème, une nouvelle approche, provenant de l'analyse des risques naturels a vu le jour dans les 25 dernières années (Weichselgartner, 2001). Il s'agit d'intégrer un nouveau paramètre dans le concept de risque, à savoir la vulnérabilité. Ce paramètre vise à intégrer, dans la notion de risque, la caractérisation du milieu et de sa sensibilité face à un aléa donné. De manière plus spécifique, il vise la considération des populations, du développement socio-économique et de l'environnement d'un secteur donné pouvant potentiellement être affectée par un aléa (Bourrelier et coll., 2000). Comme le montre la Figure 3.4, le risque est alors la combinaison de trois variables, l'aléa matérialisé par le potentiel de glissement de terrain, le système matérialisé par le village et les conséquences correspondant à l'affectation du village par l'éboulement.

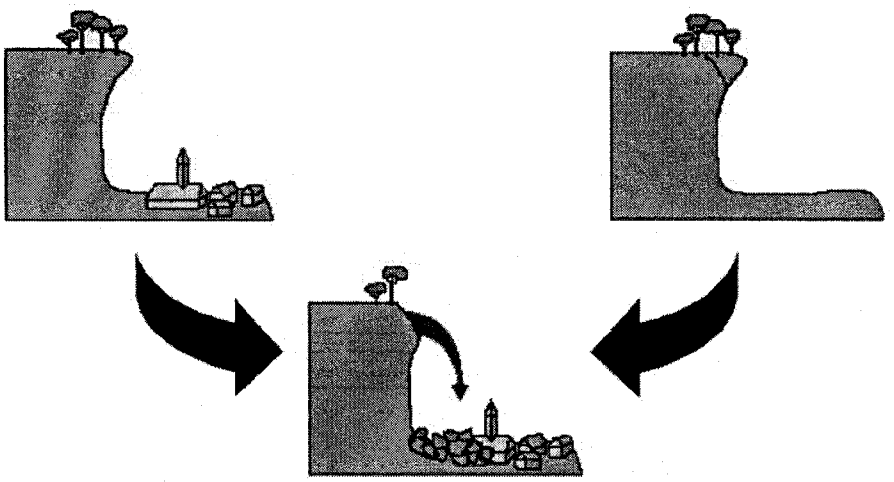

Figure 3.4 - Représentation du risque naturel (MEEDA, 2008b).

Ce concept de vulnérabilité est intéressant. Toutefois, les définitions de ce terme, à l'instar de celles du risque, sont nombreuses, comme le montre Weichselgartner (2001). Il peut donc être relativement difficile de savoir à quoi il correspond et qu'elle est sa relation avec la notion de risque. Cependant, la manière dont il est mis en œuvre, à tout le moins dans le domaine des catastrophes naturelles, fait qu'il correspond plus à la détermination d'un niveau de conséquences acceptable qu'à une nouvelle dimension du risque en lui-même. Cette approche est valable si nous nous intéressons uniquement au premier niveau de conséquences c'est-à-dire à celles qui affectent le système en tant que tel. Toutefois, il paraît important de considérer un deuxième niveau de conséquences qui, à notre avis, est prépondérant dans un contexte de sécurité civile. Il s'agit des répercussions que peuvent avoir la destruction ou la dégradation du système analysé sur son environnement.

En effet, dans un contexte de risque naturel et lorsque le système est une zone habitée, il est compréhensible de s'arrêter au premier niveau de conséquences. La sécurité civile doit intervenir à ce niveau et il n'est pas certain que les répercussions de la destruction de quelques habitations engendrent des conséquences importantes au niveau des activités socio-économiques d'une région.

Dans un contexte industriel ou en ce qui concerne les infrastructures essentielles, cela devient moins évident. En effet, la dégradation de la mission d'une infrastructure essentielle qui peut être considérée comme un premier niveau de conséquences va forcément engendrer des conséquences pour les réseaux et la société civile qui utilisent les ressources fournies par l'infrastructure essentielle. L'approche des risques naturels abordant la vulnérabilité comme étant des conséquences particulières se trouve alors inadaptée.

Dans le contexte des risques industriels, la caractérisation de la vulnérabilité fait intervenir un élément important, l'état de préparation. En effet, la vulnérabilité peut être définie comme l'état de préparation face au risque (CRAIM, 2007). Dans ce contexte, la vulnérabilité correspond donc à la préparation du système face à un aléa prédéterminé ou face à des conséquences anticipées. Cet état de préparation est donc fonction des plans de mesures d'urgence, des plans de continuité opérationnelle et des systèmes de barrières permettant de protéger le système. Il semble toutefois important d'aller plus loin dans la considération de cette notion d'état. Il ne semble pas falloir se limiter à un état de préparation qui limite l'analyse à des scénarios particuliers, mais bien considérer l'état du système dans sa globalité.

En effet, le fait qu'un aléa engendre des conséquences sur l'environnement est directement lié à l'état du système considéré et à ses zones de faiblesse. En ce sens, l'analogie avec le fromage suisse fait par Reason (2000), en ce qui a trait à la fiabilité humaine, s'applique tout à fait à la problématique des systèmes industriels (Figure 3.5).

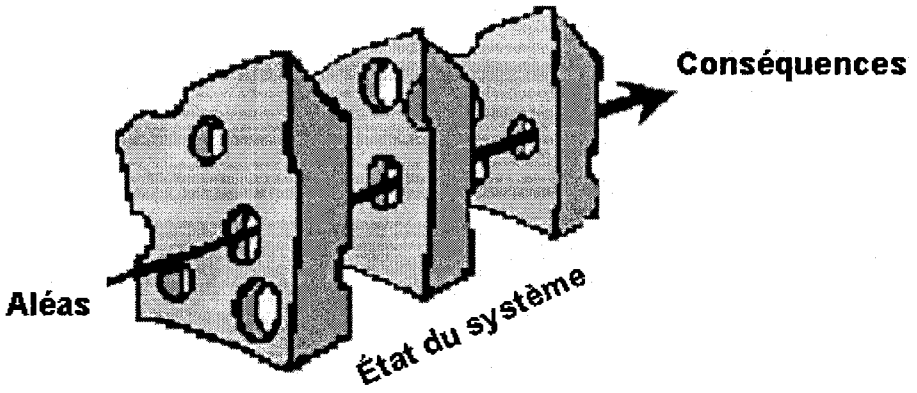

Figure 3.5 - Représentation du risque (adapté de Reason, 2000).

Comme le montre la Figure 3.5, l'aléa peut affecter le système, mais pour que des conséquences résultent de cette affectation, il faut que l'état du système le permette. Prenons l'exemple d'un barrage. De par sa conception, il peut résister à un certain niveau de crue. Si le barrage est en bon état et si les règles de gestion et d'opération sont respectées, la crue de conception ne devrait pas l'affecter et donc aucune conséquence ne devrait apparaître. Par contre, en cas d'une dégradation de l'état du barrage ou dans le cas de mauvaises applications des règles de gestion, des conséquences peuvent survenir tant pour l'ouvrage que pour son environnement, et ce, même pour une crue d'intensité inférieure à celle considérée pour la conception.

La considération de la vulnérabilité du système intégrant la prise en compte de l'état du système semble donc indispensable.

L'analyse de la vulnérabilité peut être encore raffinée. Il est en effet possible, comme l'a fait Blancher (1998), de subdiviser ce concept de vulnérabilité en ses composantes fondamentales en dissociant des vulnérabilités amont, interne et aval (Figure 3.6).

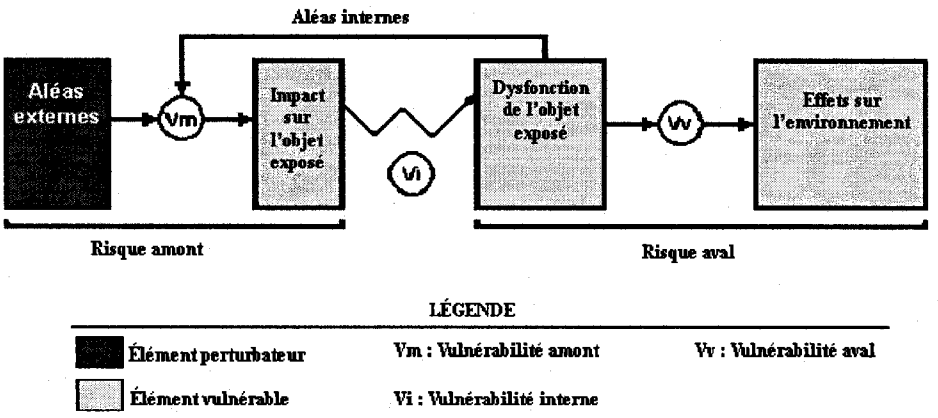

Figure 3.6 - Maillon élémentaire de la chaîne des risques (Blancher, 1998).

Cette notion de différentes vulnérabilités ou plus exactement d'une vulnérabilité composée de plusieurs variables est également intéressante. La notion d'impact sur l'objet exposé (système) et de sa dysfonction l'est tout particulièrement. En effet, la notion d'impact réfère au fait que l'aléa peut avoir un effet sur le système et prend donc en compte la notion d'état de ce système. La notion de dysfonction du système représente le premier niveau de conséquences évoqué précédemment. Le schéma présente également le deuxième niveau de conséquences représenté par les effets sur l'environnement. Un autre élément intéressant de cette figure, c'est qu'elle montre bien que plusieurs éléments peuvent être vulnérables suivant le niveau auquel s'effectue l'analyse. La vulnérabilité interne correspond à la sensibilité de l'objet exposé face à un aléa interne. La vulnérabilité aval, quant à elle, matérialise la sensibilité de l'environnement face à la défaillance de l'objet.

Toutefois, cela peut contribuer à complexifier encore plus ce concept de vulnérabilité et par le fait même le risque et son analyse. De plus, la représentation de Blancher (1998) contribue à présenter la vulnérabilité comme étant le risque. En effet, la vulnérabilité amont correspond au risque amont, la vulnérabilité interne au risque interne et la vulnérabilité aval au risque aval. Cela pourrait suggérer que la vulnérabilité est le risque et inversement.

Toutefois, cette représentation a un avantage indéniable. Plutôt que de considérer des aléas externes perturbateurs et des aléas internes, il paraît plus important de s'attarder sur les vulnérabilités tant en amont qu'internes et donc de se recentrer sur le système à l'étude. En procédant de cette façon, cela permet de définir les composantes vulnérables d'une infrastructure essentielle et de définir les moyens permettant de les renforcer.

Cependant, actuellement, bien que les notions de conséquences et de vulnérabilité soient considérées comme très importantes, l'aléa demeure au centre de la majorité des analyses de risque (Petit et coll., 2004).

Comme nous venons de le voir, il semble assez complexe de définir ce qu'est le risque. En fait, la définition du risque dépend de l'objectif de la gestion du risque et du contexte de l'étude. Par contre, certains éléments importants ressortent. Il faut donc les inclure dans une définition globale du risque. Ces éléments sont les notions d'aléa, de vulnérabilité, d'état, de système, de défaillance et de conséquences.

À partir de ces éléments, il est possible de représenter le risque grâce à ce que nous appellerons le triptyque du risque. L'objectif n'est pas de réinventer la roue ni de donner une nouvelle définition du risque pour le plaisir de le faire. Il s'agit de poser une définition du risque qui nous semble plus adéquate et que nous emploierons dans ce travail.

3.2 Le triptyque du risque

Si nous décrivons la concrétisation du risque du point de vue de l'évolution temporelle, nous avons donc la survenue d'un aléa qui va affecter un système et engendrer par la même des conséquences (Figure 3.7). Fondamentalement, pour que cette succession ait lieu, en plus de la survenue d'un aléa, il faut que le système et son état le permettent.

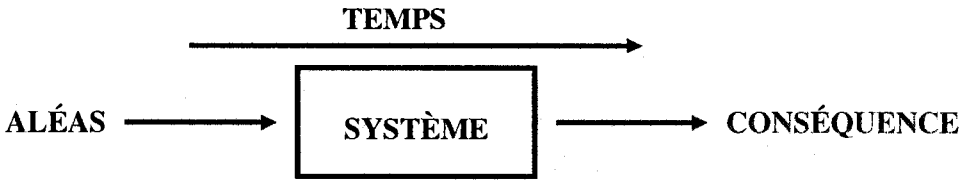

Figure 3.7 - Succession d'événements conduisant à la matérialisation du risque.

Il est possible de représenter cette succession temporelle d'événements sous forme cyclique que nous appellerons le triptyque du risque (Figure 3.8).

Cette représentation permet de faire apparaître, les trois constituants principaux permettant de caractériser le risque à savoir les aléas, l'état du système et les conséquences. Elle permet également de faire ressortir trois notions prépondérantes dans la gestion des risques : la vulnérabilité, la dysfonction et les effets domino. Le risque, dans sa globalité, est donc fonction de l'ensemble de ces six paramètres : aléas, vulnérabilité, état du système, dysfonction, conséquences et effets domino (Figure 3.8).

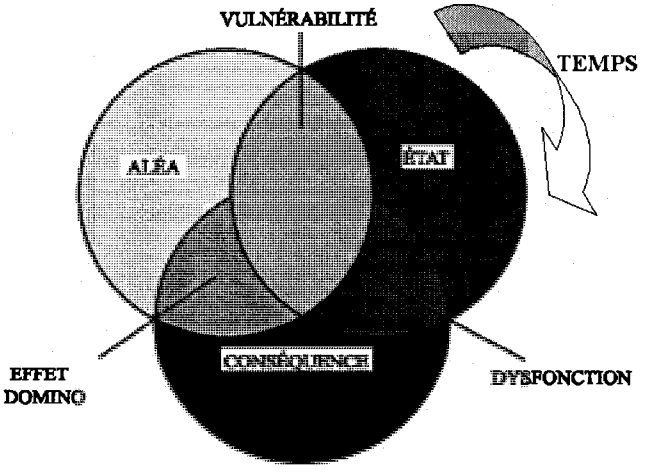

Figure 3.8 - Triptyque du risque.

À partir de la représentation de la Figure 3.8, il est donc possible de visualiser l'intégration des éléments qui constituent le risque et donc de les définir. Elle permet également de représenter la composante du temps qui est prépondérante dans le contexte de la caractérisation et de la gestion du risque.

Ce mode de représentation du risque permet également de comprendre qu'une analyse de risque peut varier suivant le contexte et la portée de l'étude qui doit être réalisée. En effet, la représentation du risque proposée permet de visualiser pourquoi tout en parlant du risque, il est possible de parler de choses différentes. Un spécialiste en mesures d'urgence va parler de gestion des risques lorsqu'il aborde la composante des conséquences sur l'environnement et d'effets domino. Un spécialiste en continuité opérationnelle, quant à lui, mettra peut être plus d'emphase sur les composantes se référant au système qu'il doit gérer à savoir les vulnérabilités, l'état et la dysfonction. L'analyse de risque et sa gestion ne sont donc pas obligées de considérer et d'intégrer l'ensemble des composantes caractérisant le risque.

Il importe donc de bien définir le contexte d'étude et les composantes du risque qui vont être prises en compte lorsque nous parlons d'analyse de risque.

Dans la définition du risque proposée, la notion d'état du système est d'autant plus intéressante en termes de continuité opérationnelle ou de mesures d'urgence qu'elle permet de caractériser une autre notion que celle de vulnérabilité, la notion de résilience.

La notion de résilience, tout comme la vulnérabilité, est une notion qui prend de plus en plus d'importance dans le cadre de la gestion des risques. De manière traditionnelle, la notion de résilience est reliée à la phase de rétablissement en mesures d'urgence. En effet, elle réfère à la capacité d'un système, d'une communauté ou d'une société à s'adapter aux perturbations découlant d'aléas, en persévérant, en récupérant ou en changeant en vue d'atteindre et de maintenir un

niveau acceptable de fonctionnement (SPC, 2007). Elle se caractérise donc comme la capacité d'un système à revenir à son état normal suite à la survenue d'aléas qui auraient affecté son mode de fonctionnement.

Par contre, à cette vision traditionnelle de la résilience, il est intéressant d'ajouter celle plus spécifique utilisée dans le domaine informatique. Dans le cas d'un système informatique, la résilience est définie comme l'aptitude à continuer de fonctionner correctement en dépit de défauts d'un ou plusieurs de ses éléments constitutifs (Grand dictionnaire terminologique, 2008). Cette façon de définir la résilience semble particulièrement pertinente si nous considérons la gestion des risques d'un point de vue continuité opérationnelle. Ces deux manières de définir la résilience sont donc importantes et doivent être considérées.

Le Tableau 3.1 présente les définitions que nous proposons et que nous utiliserons par la suite dans ce travail.

Les notions de vulnérabilité et de résilience sont complémentaires. Elles constituent les bases de l'approche actuelle en gestion des risques. En effet, de plus en plus de travaux visent à analyser la vulnérabilité d'un système de manière à en améliorer la résilience. Ces notions de même que celle de marge de manœuvre sont directement reliées à la notion d'état.

La notion d'état du système devient donc prépondérante dans toute approche de gestion des risques. De plus, cette notion d'état peut également s'appliquer pour caractériser les aléas. Ceci est particulièrement vrai pour les relations de dépendance d'un système face à l'utilisation d'une ressource donnée. Dans ce cas, l'état de la ressource peut être caractérisé comme la caractérisation du niveau de dégradation de cette ressource. Nous verrons ça plus en détail dans les prochains chapitres.

Tableau 3.1 - Définitions du risque et de ses constituantes.

Terme	Définition
Aléa	Événement d'origine anthropique ou naturelle pouvant survenir. Cet événement n'est pas forcément d'une intensité extrême. Nous ne considérons pas la notion de probabilité de survenue de l'aléa en raison de ce que nous avons expliqué précédemment.
Conséquence	Impact sur l'environnement, pris dans son sens large (biophysique, économique et social), de l'effet de la dysfonction d'un système. Il existe deux niveaux de conséquences. Les conséquences internes dont les effets se font sentir à l'intérieur du système et les conséquences externes qui affectent l'environnement du système.
Défaillance	Cessation de l'aptitude d'un système à accomplir sa ou ses missions requises avec les performances spécifiées.
Dysfonction	Altération, dégradation ou cessation de l'aptitude d'un système à accomplir sa ou ses missions requises avec les performances spécifiées.
Environnement	Contexte, ensemble des éléments naturels, humains et techniques dans lequel s'intègre le système et avec lequel il est en interaction. L'environnement du système est évolutif dans le temps.
État du système	Caractérisation de la capacité de fonctionnement des composantes d'un système. Condition d'un système. L'état du système est évolutif dans le temps.
Marge de manœuvre	Délai disponible pour mettre en œuvre les mesures de continuité opérationnelle ou de mesures d'urgence avant la défaillance du système.
Résilience	En continuité opérationnelle : Potentiel d'un système à remplir sa mission en mode défaillant. En mesures d'urgence : Potentiel d'un système à revenir à un fonctionnement normal après une défaillance.
Risque	Combinaison de l'état d'un système et de sa sensibilité face à des aléas susceptibles d'engendrer des conséquences. Le risque est donc constitué du triplet Aléas/État du système/Conséquences.
Système	Ensemble cohérent d'éléments (ou de processus) liés par des objectifs, des responsabilités ou des missions communs et fixés.
Vulnérabilité	Potentiel d'un système à être affecté par des aléas internes et/ou externes. La vulnérabilité comporte trois composantes (amont, interne et aval). La vulnérabilité du système est évolutive dans le temps.

Le système est au cœur du risque. En effet, c'est le système qui va subir les aléas et va possiblement engendrer des conséquences sur son environnement si son état ne lui permet pas soit de faire face à l'aléa soit d'éviter l'apparition de conséquences.

Il est à noter que la survenue d'un aléa externe n'est pas nécessaire pour voir se concrétiser un risque. En effet, la dégradation de l'état du système, s'apparentant à un aléa interne, pourrait à elle seule provoquer la défaillance du système et possiblement des conséquences sur l'environnement.

De manière minimale, il est possible de différencier trois types d'état pour le système considéré (Figure 3.9) :

- un état correspondant à une zone de fonctionnement normal, c'est à dire une zone dans laquelle le système est dans la capacité de remplir sa mission;
- un état correspondant à une zone de fonctionnement dégradé. Dans cet état, le système remplit encore sa mission bien que certaines de ses composantes fonctionnent de manière dégradée. La caractérisation et la connaissance de cette zone sont particulièrement importantes en termes de continuité opérationnelle ou de mesures d'urgence. En effet, il s'agit pour les gestionnaires que le système demeure le moins longtemps possible en état dégradé et que l'état normal soit rétabli. En fait, dans cet état, le système continue à remplir sa mission même si certaines de ses composantes fonctionnent dans un mode dégradé. Il est donc possible de dire que dans cet état, le système est résilient ;
- un état correspondant à une zone de fonctionnement défaillant. Dans cet état, le système ne peut remplir sa mission et des conséquences sur son environnement sont engendrées.

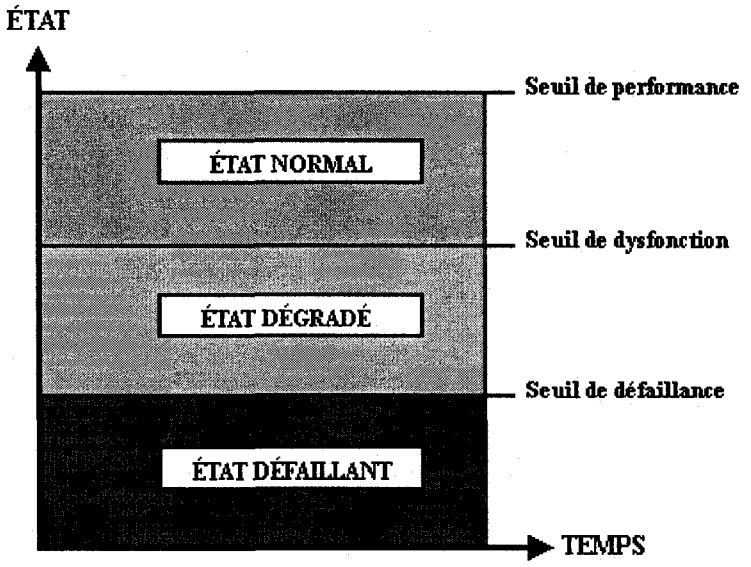

Figure 3.9 - Les états du système.

Ces trois états sont délimités par trois seuils :

- le seuil de performance. Ce seuil correspond à un niveau d'optimisation du système, à une amélioration de son efficacité ou de son rendement.
- le seuil de dysfonction. Ce seuil correspond à un niveau où certaines composantes du système vont commencer à éprouver des difficultés. Cependant, en raison des mesures palliatives ou d'atténuations, ces dysfonctions ne se répercuteront pas sur la réalisation de la mission.
- le seuil de défaillance. Ce seuil correspond au niveau à partir duquel, certaines composantes du système vont être hors service et vont donc engendrer la non-réalisation de la mission.

L'avantage de ce mode de représentation de l'état est qu'il permet de le qualifier voir de le quantifier (exemple en utilisant des pressions pour un réseau d'eau potable) et de considérer son évolution en fonction du temps. Il est évident que les largeurs des trois zones d'état vont varier suivant le système étudié. De plus, la succession des états possibles peut varier également. En effet, suivant le système

considéré, il est possible qu'il existe plusieurs seuils de dysfonction et de défaillance (Figure 3.10).

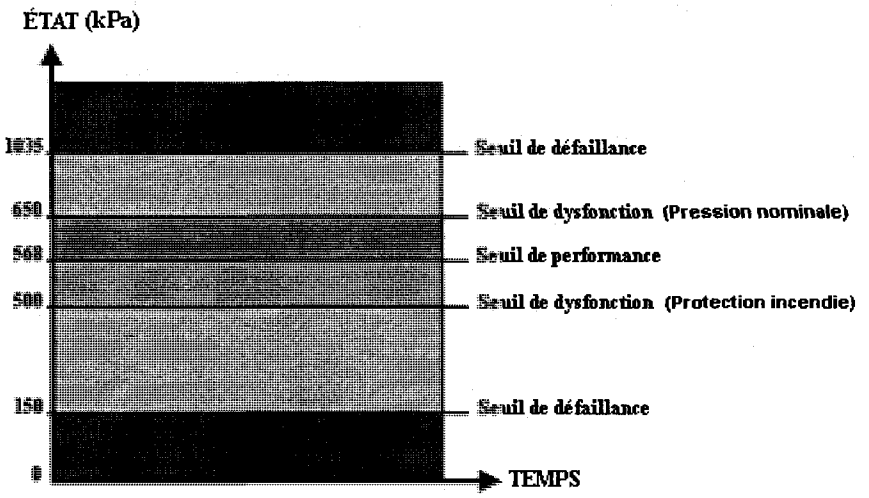

Figure 3.10 - États pour une conduite d'eau potable.

La Figure 3.10 illustre donc un autre enchaînement possible d'états pour un système. Cette figure est basée sur les pressions d'eau nécessaires pour la protection incendie d'un bâtiment de quatre étages. Elle caractérise donc l'état d'un réseau d'eau potable en relation avec une de ses missions qui est de fournir de l'eau pour la protection incendie. Les états possibles du système sont délimités en termes de pression d'eau nécessaire pour cette protection, mais également en termes de pression pouvant être supportée par les conduites du réseau d'eau.

Il existe deux zones de défaillance qui vont avoir pour conséquences la non-possibilité de protéger le bâtiment considéré contre un incendie. La première zone entre 0 et 150kPa correspond à une pression insuffisante pour la protection incendie. En effet, 150kPa correspond au débit à réserver pour la sécurité incendie (Bonneville, 1999). La deuxième zone est délimitée par la pression nominale maximale des systèmes de distribution publique d'eau (Bonneville, 1999). La pression nominale correspond à la pression d'eau intérieure maintenue constante,

que l'élément de canalisation doit supporter sans défaillance et avec une sécurité convenable.

Il existe également deux zones de dysfonction. La première entre 150 et 500kPa (pression minimale recommandée à l'entrée des bâtiments). La deuxième entre 650kPa (pression maximale d'opération optimale du réseau) et 1035kPa (pression nominale maximale du réseau).

Finalement, la dernière zone correspond à la zone optimale de fonctionnement. Elle est située entre 568 et 650kPa. En effet, 568kPa correspond à la pression nécessaire pour la protection incendie d'un bâtiment de quatre étages.

Une fois définie la succession des états possibles d'un système, il s'agit de caractériser comment se fait le changement d'état pour ce système. Cette variation de l'état de fonctionnement du système est directement influencée par les aléas tant externes qu'internes de même que par l'effet du temps.

La caractérisation de l'état du système permet donc de faire le lien entre les aléas et les conséquences engendrées sur l'environnement (Figure 3.11), mais aussi de caractériser sa vulnérabilité et sa résilience. En caractérisant l'évolution de l'état du système en fonction du temps, il est également possible de définir une marge de manœuvre, qui correspond au délai disponible avant que le système entre en défaillance.

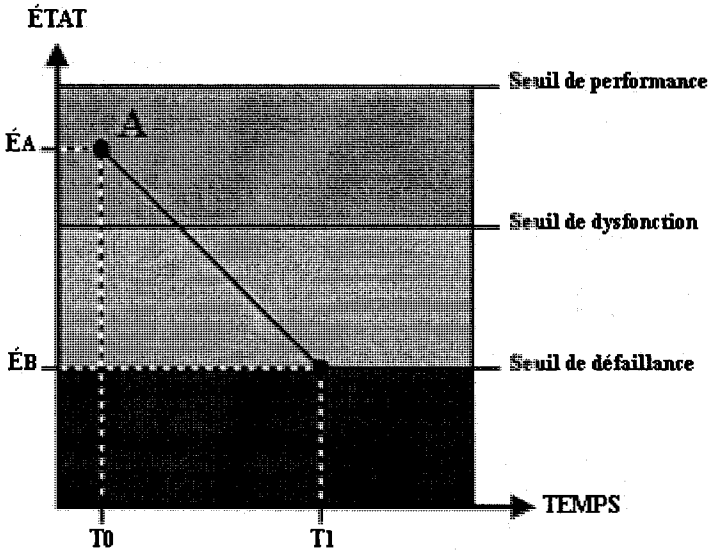

Figure 3.11 - Visualisation de la variation d'état du système.

Considérons le système comme étant à un état normal $É_A$ au temps T_0 (point A sur la Figure 3.11). L'usure normale du système le conduira à atteindre un état défaillant $É_B$ au temps T_1 (point B sur la Figure 3.11).

Ceci est d'autant plus vrai si nous considérons une composante précise du système, telle qu'une infrastructure ou un équipement. Quelles que soient les mesures prises, l'état d'une infrastructure va forcément se dégrader en fonction de la durée de son utilisation. Le délai séparant T_0 de T_1 correspond à la marge de manœuvre maximale dont dispose le système entre le moment de son entrée en service et le moment où il sera défaillant en raison de son âge.

Cette durée d'utilisation peut être complexe à définir pour un système dans son ensemble, mais est relativement facile à obtenir pour les infrastructures qui le composent. L'évolution de l'état d'une infrastructure peut être définie dès sa conception en considérant une utilisation normale. En effet, dans la majorité des cas, le mode d'emploi d'un équipement ou la mise en service d'une infrastructure définit un état optimal de fonctionnement de même qu'une durée de vie utile.

Le niveau de l'état de défaillance est également défini dès la mise en fonctionnement d'une infrastructure. En effet, ce niveau correspond à la mise hors service de cette infrastructure ou au moment où son fonctionnement sera désuet.

En conséquence, dès la mise en fonctionnement d'un système, il est possible de définir :

- son état optimal de fonctionnement ($É_A$ sur la Figure 3.11) ;
- l'état correspondant à la mise hors service du système ($É_B$ sur la Figure 3.11) ;
- la durée de vie utile du système correspondant à la marge de manœuvre de conception (T_1-T_0 sur la Figure 3.11).

Il est donc possible de produire la droite représentée sur la Figure 3.11, toutes les données permettant de la tracer étant connues.

La détermination de cette droite permet également de déterminer une autre information prépondérante pour la continuité opérationnelle et les mesures d'urgence à savoir sa pente (p) :

$$p=\frac{É_B-É_A}{T_1-T_0} \qquad (1)$$

d'où

$$p=\frac{Variation\cdot d'état}{Marge\cdot de\cdot manoeuvre} \qquad (2)$$

La variation d'état peut être déterminée dès la conception du système. En effet, les états tant de fonctionnement optimal que celui menant à la défaillance du système peuvent être définie en se basant sur la qualité de service et donc sur l'utilisation qui sera faite de la ressource fournie par le système. Il devient donc intéressant d'évaluer une variation possible de la pente de la droite obtenue, car elle permettra de définir la marge de manœuvre disponible pour le gestionnaire du système avant la défaillance de celui-ci. La Figure 3.12 représente l'évolution anticipée de l'état du système en fonction du temps. Cette figure est obtenue en s'alignant le long de

la droite figurant le passage de l'état A à l'état B. La marge de manœuvre correspond donc au délai disponible et anticipé séparant l'état actuel du système du moment où le système va se retrouver dans un état défaillant ou hors service. Cependant, cette approximation ne permet pas véritablement de définir avec précision la largeur de la zone d'état dégradé ou zone de dysfonction du système. Il serait intéressant de pouvoir mieux caractériser cette zone, car elle correspond en fait à la résilience du système quant elle est abordée sous l'angle de la capacité de fonctionner en état dégradé.

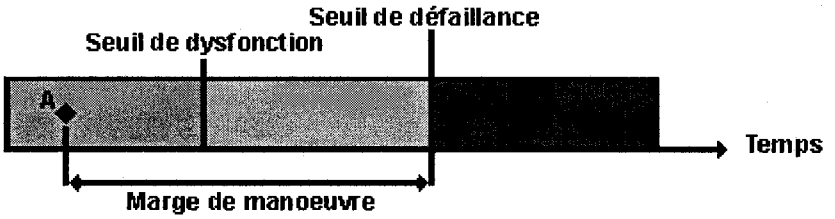

Figure 3.12 - Évolution de l'état du système en fonction du temps.

L'intérêt de la Figure 3.12 est qu'elle permet de représenter de manière visuelle la marge de manœuvre à la disposition du gestionnaire du système avant qu'il n'entre en défaillance. Si le système est dans l'état A, la marge de manœuvre est le délai (variation de temps qui existe entre le point A et le seuil de défaillance). En déterminant le type de l'évolution des états possibles ainsi que l'état actuel d'une composante d'un système, il est donc possible de déterminer une marge de manœuvre qui est prépondérante dans un contexte de mesures d'urgence et de continuité opérationnelle.

Plus la pente de la droite de la Figure 3.11 est importante, plus la marge de manœuvre, dont dispose le gestionnaire avant la défaillance du système, sera courte. En effet, l'augmentation de la pente va contribuer à réduire la taille de la zone de dysfonction et par conséquent le délai séparant l'état normal de l'état de défaillance. Au contraire, plus la pente sera faible et plus la marge de manœuvre sera importante.

Cette pente va varier en fonction des aléas qui vont affecter le système, mais aussi en fonction des mesures (barrières) mises en œuvre pour protéger le système (Figure 3.13). Elle constitue en cela un outil d'aide à la décision important pour maintenir le système en état de fonctionnement. En effet, les aléas vont directement affecter le système s'il est vulnérable.

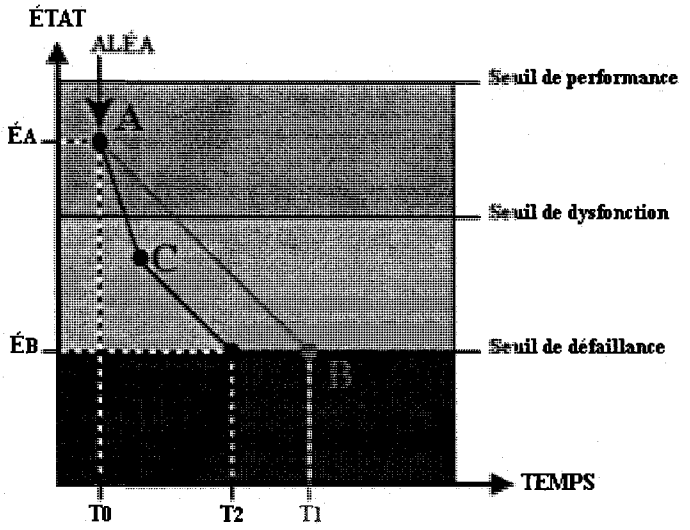

Figure 3.13 - Variation de la pente de dégradation.

Dans la Figure 3.11, seule la variation d'état due à la l'usure normale d'une composante du système a été considérée. Cependant, l'état de la composante va également varier en fonction des aléas qui peuvent potentiellement affecter la composante. La Figure 3.13 montre un exemple possible de cette variation. Au temps T_0, la composante considérée se situe en A. Le vieillissement anticipé de la composante fait qu'au temps T_1, la composante devrait atteindre l'état B et donc entrer en défaillance. Cependant, au temps T_0, la composante est affectée par un aléa qui va accélérer sa dégradation. La composante va rapidement atteindre un état C. La composante sera alors dysfonctionnelle, mais non défaillante. Par la suite, l'effet de l'usure de la composante va contribuer à augmenter la dégradation de la composante jusqu'à l'atteinte de sa défaillance en D au temps T_2. La survenue de

l'aléa fait donc que la composante du système va être défaillante au temps T_2 au lieu du temps T_1. L'aléa a un effet sur la pente de dégradation et va, par conséquent, affecter le délai disponible avant la défaillance de la composante. La Figure 3.14 présente la nouvelle marge de manœuvre dont dispose le gestionnaire du système en cas de survenue de l'aléa pouvant engendrer une variation de la pente de dégradation, tel que vu dans la Figure 3.13.

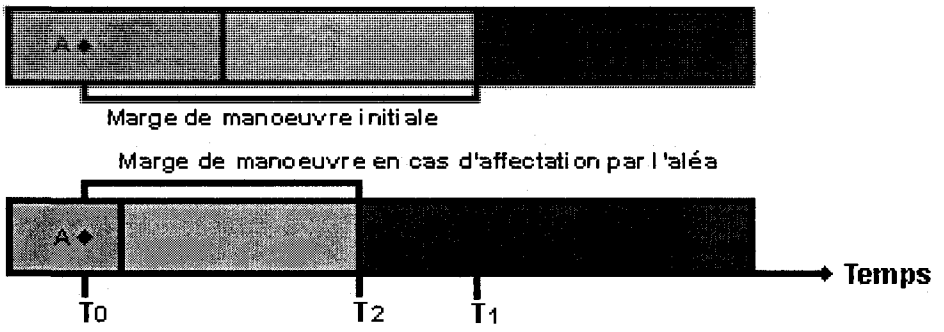

Figure 3.14 - Comparaison des marges de manœuvre.

La Figure 3.14 montre que la survenue d'un aléa qui engendrerait le passage de l'état A à un état C puis D de la composante (Figure 3.13) provoquerait un rétrécissement des zones d'état normal et d'état de dysfonction. Cela provoquerait une diminution du délai séparant la composante de sa zone de défaillance. Le gestionnaire du système verrait donc sa marge de manœuvre lui permettant de s'adapter à la situation diminuée.

Dans les exemples précédents, l'évolution de l'état du système a été considérée comme étant linéaire et continue. Cela est un peu plus complexe dans le sens que cette évolution peut prendre différente forme et être discrète. Cependant, il sera sans doute toujours possible d'approximer l'évolution de l'état du système par une droite pour laquelle une pente pourra être calculée et par le fait même de déterminer une marge de manœuvre. D'autre part, il s'agit plus d'avoir une idée de l'évolution de l'état du système de manière à prendre les actions qui s'imposent. Il

n'est pas forcément nécessaire de modéliser très finement l'évolution de cet état. En fait, tout dépend de l'objectif de l'analyse des risques effectuée.

Cette façon de faire permettra de lever une partie de l'incertitude entourant l'évolution de l'état d'un système. Il est également possible de penser que les principes de la logique floue pourraient également être utiles. En effet, il s'agit plus de lever une part d'incertitude en développant un outil d'aide à la décision plutôt que d'essayer de prévoir l'imprévisible. Il faut donc déterminer l'allure de l'évolution de l'état des composantes du système et donc du système par rapport à un niveau de référence. Ce niveau de référence peut être caractérisé par les droites présentées à la Figure 3.13 et surtout par leur pente.

Il est évident que cette approche semble relativement simple d'un point de vue théorique, mais qu'elle peut se révéler nettement plus complexe à appliquer en pratique. Ceci est d'autant plus vrai si nous prenons en compte le côté opérationnel d'un système. En effet, il semble plus facile de caractériser l'état d'une infrastructure ou d'un équipement que celui d'une fonction ou une activité.

D'autre part, les actions prises par le gestionnaire vont directement influer sur le mode de variation de l'état de chacune des composantes du système. En effet, les opérations d'entretien, de contrôle et de surveillance de même que les mesures de prévention, de protection et d'intervention vont, comme les aléas, provoquer des changements. Ces changements devraient se concrétiser par une augmentation de la marge de manœuvre à la disposition du gestionnaire de l'infrastructure essentielle. Tout comme les effets des aléas, les effets potentiels des mesures mises en place pour les contrer ne vont pas forcément se traduire par une évolution linéaire et continue.

Toutefois, cette difficulté peut être levée en se focalisant sur les seuils de dysfonction et de défaillance qui constituent les éléments indispensables à toute prise de décision dans les domaines des mesures d'urgence et de continuité

opérationnelle. Le moment du passage des seuils est particulièrement important. En effet, le passage du seuil de dysfonction est prépondérant en termes de continuité opérationnelle. Il délimite la zone pour laquelle le plan de continuité opérationnelle doit être appliqué pour éviter la défaillance. Les seuils de changement d'état ne sont pas forcément associés à des valeurs précises. Dans le cas présenté à la Figure 3.10, les seuils ont été déterminés en leur attribuant des valeurs de pression. Toutefois, il est fortement possible que le changement d'état s'effectue un peu avant ou un peu après ces valeurs seuils. Il faut donc en fait déterminer des zones de transition (Figure 3.15). Pour cela, il est possible de combiner les résultats obtenus à l'aide des Figures 3.13 et 3.14.

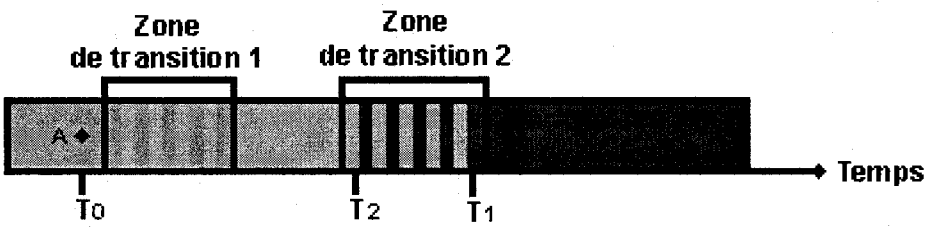

Figure 3.15 - Variation des états avec les zones de transition.

Deux zones de transitions peuvent être définies. La zone de transition 1 entre l'état normal et l'état de dysfonction. Cette zone commence un peu avant le seuil qui résulterait d'une usure normale de la composante et se termine un peu après le seuil de dysfonction qui résulterait de la survenue d'un aléa. La zone de transition 2 se situe entre l'état de dysfonction et l'état défaillant. Cette zone débute avant le temps T_2 et se termine un peu après l'état T_1.

La constitution de figures, telle que la Figure 3.15, associée à des systèmes d'alerte lorsque l'état s'approche d'une zone de transition ou en mettant en place des opérations de veille particulières contribuera sans aucun doute à une meilleure gestion des systèmes en favorisant une approche proactive des risques. Il faut pour cela construire ces figures avant la survenue d'événements de manière à pouvoir anticiper l'évolution possible du système.

Toutefois, la création de telles courbes peut s'avérer complexe si l'objectif est de calculer de manière précise l'évolution possible d'un système. Il s'avère peut-être plus judicieux de déterminer ces courbes en se basant sur les jugements d'experts spécialistes des systèmes analysés. Il s'agit en fait de déterminer une tendance d'évolution possible de l'état du système de manière à se préparer à intervenir lors de la survenue d'un aléa.

3.3 Application des concepts proposés

Les concepts proposés sont actuellement appliqués tant à un niveau stratégique qu'à un niveau opérationnel.

À un niveau stratégique, les définitions proposées tant pour le risque que pour la résilience sont utilisées par le gouvernement du Québec pour favoriser la résilience des systèmes essentiels. Pour ce faire, l'Organisation de sécurité civile du Québec (OSCQ) se base sur les notions de variations d'état (normal, dégradé et défaillant) des systèmes gouvernementaux. Une fois ces états possibles définis, il s'agit donc de favoriser la résilience des systèmes. Pour cela, les deux variantes de la résilience que nous proposons sont employées. La résilience est en effet vue comme la capacité d'un système à maintenir ou à remplir un niveau de fonctionnement acceptable malgré les défaillances (Neault, 2009). Les travaux de l'OSCQ sont encore à un niveau d'appropriation des concepts que nous proposons.

Le concept de vulnérabilité n'est pas encore véritablement utilisé à tout le moins comme nous le définissons. Cependant, ce concept de vulnérabilité est intimement relié à la notion d'état du système. De ce fait, lorsque nous considérons la variation d'état d'un système, nous étudions obligatoirement la vulnérabilité du système. Il est logique de penser que la dégradation de l'état d'un système augmentera obligatoirement sa vulnérabilité face à différents dangers qui ne l'auraient pas affecté s'il avait été dans un état normal. Toutefois, il n'en demeure pas moins que la majorité des définitions, que nous proposons, sont véritablement à la base de la démarche du gouvernement du Québec pour la résilience des systèmes. De plus, les

travaux futurs, visant à améliorer la résilience des systèmes essentiels au Québec, passent par le développement d'un Guide méthodologique d'évaluation de la résilience d'un système essentiel (Neault, 2009). Ce guide, qui se base sur les concepts que nous proposons, est actuellement en développement par le *Centre risque & performance* de l'École Polytechnique de Montréal.

Les concepts de définition du risque proposés sont également utilisés à un niveau opérationnel. Ces concepts sont à la base de nombreux travaux réalisés par le *Centre risque & performance* pour la ville de Montréal, capitale économique de la province de Québec, et pour la ville de Québec, capitale politique de la province de Québec (Robert and Morabito, 2008). En effet, ces travaux utilisent notamment la notion de variation d'état du système pour développer des courbes de dépendance des infrastructures essentielles,

La Figure 3.16 présente un exemple de graphique de dépendance obtenu pour la ville de Montréal.

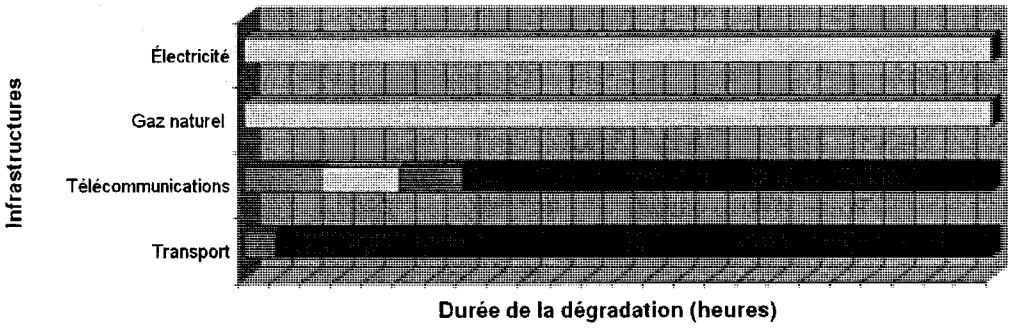

Figure 3.16 - Courbes de conséquences d'un problème d'alimentation en eau (Robert and Morabito, 2008)

La Figure 3.16 présente les variations d'état de quatre infrastructures essentielles (électricité, gaz naturel, télécommunications et transport) en relation avec un arrêt de l'alimentation en eau potable. Cette courbe montre que la perte de l'alimentation

en eau potable va se traduire par une défaillance (mise hors service) des réseaux de transport et de télécommunications après une certaine durée de dégradation.

Le réseau de télécommunications a besoin d'eau pour le refroidissement de certains de ses équipements. La perte de l'alimentation en eau pourrait donc se traduire après un certain temps par la dysfonction du réseau de télécommunications et ultimement par sa mise hors service.

Le réseau de transport a besoin d'eau pour des raisons de sécurité incendie. En cas de perte de l'alimentation en eau, les procédures de sécurité incendie oblige de fermer certains axes routiers, tels que les tunnels. La mise hors service du réseau de transport est donc pratiquement immédiate en cas d'arrêt de la fourniture d'eau potable.

Les deux autres réseaux (électricité et gaz naturel) présents sur la zone d'étude ne sont pas véritablement dépendants de l'eau potable pour ce qui est de leur fonctionnement technique. En effet, la perte de l'alimentation en eau n'engendre pas un état de dysfonctionnement pour ces deux infrastructures essentielles.

Il est évident que le graphique de dépendance de ces réseaux par rapport à l'utilisation de l'eau potable serait différent si nous prenions en compte la non-portabilité de l'eau. À ce moment-là, il faudrait considérer, l'utilisation de l'eau pour la consommation humaine. Les variations d'états des systèmes seraient alors différentes, de même que les délais disponibles avant la défaillance des quatre infrastructures essentielles considérées.

Ces utilisations concrètes des concepts proposés pour définir le risque permettent de vérifier notre première hypothèse de travail qui stipulait qu'il fallait considérer l'état d'un système et par le fait même sa vulnérabilité de manière à pouvoir effectuer une analyse des risques.

3.4 Conclusion

Ce chapitre a permis de poser les bases de notre travail en proposant une définition des risques intégrant les paramètres généralement considérés tels que les aléas et les conséquences et en faisant ressortir la notion d'état du système. En cela, nous atteignons le premier objectif de ce travail qui était de définir les concepts de risque et de vulnérabilité. Cette manière de définir le risque permet également de faire ressortir les notions de vulnérabilité, de dysfonction et d'effet domino qui sont prépondérantes dans le cadre de systèmes de plus en plus interconnectés. Cette manière de définir le risque semble applicable, quel que soit le contexte d'étude, et est particulièrement adaptée à la problématique des interdépendances entre infrastructures essentielles comme l'ont montré les travaux effectués par le *Centre risque & performance* pour les villes de Montréal et de Québec.

Nous avons également vu que les concepts proposés sont utilisés pour supporter le développement d'une méthodologie, qui vise à favoriser la résilience des systèmes essentiels, qui est actuellement en développement par le gouvernement du Québec.

Ce chapitre, par l'atteinte de notre premier objectif, permet de vérifier notre première hypothèse de travail à savoir que le concept de vulnérabilité et la notion d'état d'un système sont des composantes intrinsèques du risque. Il a permis d'introduire également les notions de résilience et de marge de manœuvre qui sont de plus en plus importantes dans le domaine des risques. Il a également abordé la notion de zone de transition qui peut se révéler prépondérante dans un contexte de gestion des risques.

Il apparaît donc important de poser les bases d'une méthodologie d'analyse des risques qui intègre ces notions de vulnérabilité et d'état du système. Cette méthodologie doit également être adaptée aux infrastructures essentielles et intégrer leurs particularités. Le chapitre suivant présente la méthode que nous proposons pour caractériser une infrastructure essentielle de manière à pouvoir, par la suite, poser les bases d'une méthode d'analyse de ses vulnérabilités.

CHAPITRE 4 ORGANISATION D'UNE INFRASTRUCTURE ESSENTIELLE

Nous avons vu dans le chapitre précédent que les notions de vulnérabilité et de résilience d'un système sont prépondérantes dans le cadre de la gestion des risques et ceci d'autant plus si nous nous basons tant du point de vue des mesures d'urgence que de celui de la continuité opérationnelle. Ces deux notions de vulnérabilité et de résilience sont directement liées à l'état du système sur lequel porte l'analyse de risque. Il faut donc pouvoir caractériser le système à l'étude de manière à pouvoir analyser son état. Dans ce travail, le système est une infrastructure essentielle.

Le présent chapitre a donc pour but de voir comment caractériser une infrastructure essentielle de manière à faire ressortir les éléments qui permettraient d'analyser ses vulnérabilités, et par la même, les risques qui sont associés à son fonctionnement.

Dans un premier temps, nous verrons le mode d'organisation d'une infrastructure essentielle de même que les particularités qui peuvent la caractériser. Il est important de considérer également les notions d'interdépendances entre infrastructures essentielles tant cette problématique est d'actualité.

Dans un deuxième temps, nous poserons les bases permettant la caractérisation d'une infrastructure essentielle en intégrant les éléments nécessaires à la détermination du risque tel que défini dans le chapitre précédent.

4.1 Organisation et interdépendance entre infrastructures essentielles

Les infrastructures essentielles sont des réseaux relativement complexes en raison de leur organisation. Elles sont constituées d'un ensemble de composantes formant des systèmes principaux, primordiaux pour le fonctionnement du réseau, et secondaires, utiles pour ce fonctionnement. D'ailleurs, les intervenants commencent à définir les infrastructures essentielles comme des systèmes critiques pour le fonctionnement de la société (SPC, 2008b). L'ensemble forme une structure

intégrée dont la fiabilité est dépendante de l'efficacité de l'ensemble de ses constituants. De plus, dans la majorité des cas, les composantes des infrastructures essentielles s'étendent sur de grandes zones géographiques ce qui rend leur analyse d'autant plus complexe. L'approche classique d'analyse des risques axée sur la considération de différents aléas servant à élaborer des scénarios d'affectation d'un système est peu adaptée à ce type complexe d'organisation. Ceci pour deux raisons. La première est due à l'étendue géographique. En effet, il est peu réaliste d'analyser l'ensemble des aléas pouvant affecter un réseau à l'échelle d'une province ou d'un pays. La deuxième est due à l'organisation de ces infrastructures essentielles. En effet, un aléa peut affecter un réseau dans un secteur sans que les conséquences engendrées ne se fassent ressentir dans ce même secteur. Les conséquences peuvent se concrétiser dans un endroit où l'aléa ne s'est pas produit.

Une manière d'aborder la caractérisation d'un système complexe, tel qu'une infrastructure essentielle est de se focaliser sur sa mission, le but pour lequel elle a été développée. Fondamentalement, les infrastructures essentielles sont mises en place pour répondre à des besoins précis de la société. De plus, il est possible de considérer dans une première approche qu'une infrastructure essentielle est construite pour répondre au besoin d'une autre infrastructure essentielle. Cette manière d'aborder l'organisation des infrastructures essentielles la rend certainement plus simple à caractériser. Dans ce contexte, une municipalité doit elle-même être considérée comme étant une infrastructure essentielle qui apporte un soutien et des services à la population.

Une autre problématique à considérer est les interconnexions entre infrastructures essentielles et donc les défaillances en cascade que peut engendrer le dysfonctionnement d'une de ces infrastructures essentielles. Cette problématique peut également être abordée relativement simplement si nous considérons qu'une infrastructure essentielle va produire un bien ou un service qui sera utilisé par une autre infrastructure essentielle. Cette manière d'aborder le problème permet sans aucun doute de considérer les liens physiques entre infrastructures essentielles. Elle

peut également servir pour l'étude des liens cybernétiques et des liens logiques. L'approche doit toutefois être différente en ce qui concerne les liens géographiques qui n'ont aucune réalité physique avant la défaillance d'un réseau. Leur analyse nécessite d'aborder le problème en intégrant la localisation des composantes des infrastructures essentielles.

4.2 Caractérisation d'une infrastructure essentielle

La question que nous pouvons nous poser est comment caractériser ou représenter une infrastructure essentielle de manière à :

- faire ressortir ses particularités ;
- pouvoir analyser ses vulnérabilités ;
- pouvoir contribuer à son renforcement et à sa protection.

D'après la définition que nous avons donnée du risque dans le chapitre précédent, nous devons trouver une représentation des infrastructures essentielles permettant de faire ressortir les six composantes du risque (aléas, vulnérabilité, état, dysfonction, conséquences, effets domino).

Pour cela, il est nécessaire de s'intéresser au mode organisationnel des infrastructures essentielles. Il est évident que chaque infrastructure essentielle, suivant son secteur d'activité, peut présenter des particularités. L'objectif est de définir un mode d'organisation commun qui pourrait servir de support à l'élaboration d'une méthodologie d'analyse de risque.

De manière minimale, la première chose commune, entre différentes infrastructures essentielles, est qu'elles sont élaborées pour combler un ou des besoins. De ce fait, il est possible de déterminer une ou des missions qu'elles doivent remplir. La mission d'une infrastructure essentielle peut s'exprimer en termes de fourniture d'une ressource. D'ailleurs, il est possible de définir une mission comme la raison d'être d'un système. Elle vise donc la fourniture d'une ressource avec des caractéristiques précises.

Si la ressource ou les caractéristiques de fourniture changent alors la mission n'est plus la même. Il est possible de parler de mission première ou principale pour les missions d'un système qui se réfèrent à la fourniture d'une ressource. Il existe d'autres types de mission secondaires ou de soutien qui sont plus liés au fonctionnement et à la protection des systèmes et de leur environnement. Ces missions peuvent être définies en fonction des réglementations et des normes que doivent respecter les infrastructures essentielles lors de leurs opérations. Dans ce cas, il n'est plus vraiment possible de parler de fourniture, un autre verbe d'action devra être utilisé.

Le Tableau 4.1 présente quelques-unes de ces missions pour différentes infrastructures essentielles.

Les missions des réseaux peuvent donc être caractérisées dans la majorité des cas comme la fourniture d'une ressource avec des caractéristiques pouvant être quantifiables ou, à tout le moins, qualifiables. Par exemple, pour un aqueduc, il est relativement aisé d'analyser (quantifier) la réalisation correcte de la mission de distribution d'eau potable, les paramètres caractérisant la ressource fournie (eau) étant mesurables. En effet, il est possible de caractériser la mission de fourniture d'eau potable en mesurant, par exemple, le volume d'eau qui arrive à un point donné. De plus, ce volume d'eau à fournir peut être défini par réglementation, en particulier si nous considérons la problématique de la protection incendie. Il est également possible d'utiliser des paramètres de mesure pour caractériser la qualité de l'eau distribuée. Les paramètres utilisés, pour déterminer si une eau est potable ou non, sont relativement bien définis étant donné qu'ils sont, pour la majorité, imposés par la réglementation. Toutefois, lorsque nous considérons la notion de qualité de l'eau, il faut combiner plusieurs paramètres tels que les matières en suspension, la turbidité, l'alcalinité ou encore la demande biologique en oxygène. Donc, cela peut rendre les choses un peu plus complexes, car il n'est pas possible d'utiliser un critère unique et simple pour caractériser la mission. Il faut plutôt

utiliser un indice qui va combiner plusieurs critères. La problématique de savoir comment combiner ces critères se pose alors.

Tableau 4.1 - Missions de différentes infrastructures essentielles.

Infrastructures essentielles	Missions
Aqueduc	• **Fournir de l'eau** avec certaines caractéristiques de **pression** pour la protection incendie. • **Fournir de l'eau** avec certains critères de **qualité** pour l'alimentation en eau potable. • **Fournir de l'eau** avec certaines caractéristiques de **volume** ou de **température** pour le fonctionnement d'équipement.
Électricité	• **Fournir de l'électricité** avec certaines caractéristiques de **voltage.** • **Fournir de l'électricité** avec certaines caractéristiques de **qualité de l'onde.** • **Assurer un débit réservé minimal** avec certaines caractéristiques de **volume** d'eau lors de l'opération d'un barrage.
Transport	• **Assurer** une qualité de la surface de roulement. • **Assurer** la sécurité des usagers. • **Assurer** une certaine fluidité dans les déplacements.
Télécommunications	• **Fournir** une bonne **qualité de service** aux utilisateurs du réseau en termes de **délai de connexion** ou de **qualité de transmission.** • **Assurer** une bonne **qualité de fonctionnement** du réseau en termes de **nombre de pannes**.

Les critères qui permettraient de caractériser les missions des réseaux de transport ou de télécommunications sont plus difficiles à déterminer et, par la même, à quantifier. Ceci est dû au fait que ce sont des infrastructures essentielles qui mettent leur réseau à la disposition de leurs usagers pour supporter les activités de ces derniers. Il n'y a pas véritablement de bien ou de matière fournis.

De manière générale, il est tout de même toujours possible d'associer à la mission d'une infrastructure essentielle, une ressource qui sera utilisée par une autre infrastructure essentielle. La dysfonction du réseau peut donc être caractérisée comme la dégradation de sa mission et donc l'affectation des critères caractérisant la ressource qu'il doit fournir.

Comme le montre Robert et coll. (2007), il est possible de différencier de manière générale six types principaux de ressources (Tableau 4.2).

Tableau 4.2 - Types de ressources (Robert et coll., 2007).

Type de ressource	Définition
Infrastructure/équipement	Ouvrage, installation, bâtiment, équipement majeur.
Matière/énergie/bien	Substance physique.
Humaine	Personnel nécessaire au fonctionnement du système.
Information/donnée	Renseignement, indication, donnée.
Financière/assurance	Capital, crédit, assurance.
Service	Expertise. Fonction d'utilité commune. Fourniture d'un bien immatériel.

Comme nous avons spécifié que les ressources sont produites et utilisées par des infrastructures essentielles, ce sont elles qui permettent véritablement de

caractériser les liens et donc les interdépendances entre infrastructures essentielles. Il est donc possible de considérer le système à l'étude comme une boîte noire dans laquelle entrent des ressources et de laquelle ressortent d'autres ressources (Figure 4.1).

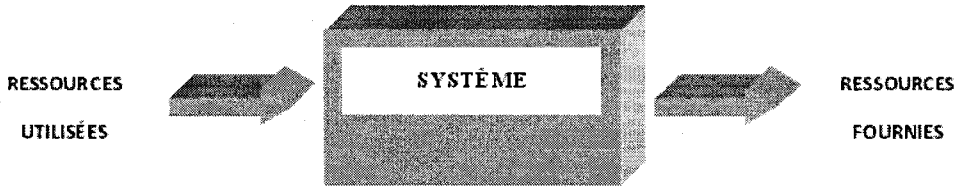

Figure 4.1 - Le système, un fournisseur et un utilisateur de ressources.

Cette manière de considérer une infrastructure essentielle peut s'avérer suffisante si nous abordons le risque du point de vue des mesures d'urgence. En effet, il n'est pas nécessaire de connaître les opérations réalisées à l'intérieur de l'infrastructure essentielle. Il suffit de connaître les répercussions de la défaillance de l'infrastructure essentielle sur son environnement et donc de savoir si la ressource fournie par le système est dégradée ou non. Cette approche est suffisante également pour l'étude des effets domino entre infrastructures essentielles. En effet, nous avons dit que la connaissance des ressources utilisées et fournies était suffisante pour caractériser les liens de dépendances. Si nous décidons d'aborder le système comme étant une boîte noire, il suffit alors d'effectuer une analyse fonctionnelle externe ce qui permettra de se focaliser sur les ressources entrant et sortant du système.

Par contre, la considération du système en boîte noire ne permet pas vraiment d'aborder le risque du point de vue de la continuité opérationnelle. En effet, dans ce cas, il est important de pouvoir caractériser d'autres composantes du risque tel que l'état de l'infrastructure essentielle considérée. Pour cela, il faut détailler un peu plus le processus se déroulant au sein du système et donc au sein de l'infrastructure essentielle sur laquelle porte l'analyse.

De manière minimale, il est possible de définir l'organisation interne d'une infrastructure essentielle comme un regroupement de fonctions, d'opérations et d'infrastructures. En effet, toute infrastructure essentielle est composée d'infrastructures. C'est même la première chose à laquelle nous pensons quand nous parlons d'infrastructure essentielle. Ces infrastructures peuvent être de natures diverses. Le Tableau 4.3 présente des exemples d'infrastructures pour un réseau d'électricité.

Tableau 4.3 - Exemples d'infrastructures constituant un réseau d'électricité.

Infrastructures	Fonctions
• Centrale hydroélectrique ; • Centrale nucléaire ; • Parc éolien ; • Centrale thermique.	**Production**
• Lignes de transport de 765 kilovolts ; • Transformateur.	**Transport**
• Ligne de distribution de 750 volts ; • Centre de contrôle du réseau.	**Distribution**

Comme le montre le Tableau 4.3, les infrastructures qui constituent le tissu de l'infrastructure essentielle sont mises en place pour soutenir une fonction. Une centrale hydroélectrique va servir pour remplir une partie de la fonction de production du réseau électrique. Un deuxième élément organisationnel d'un système ressort donc, il s'agit de la fonction.

Il est possible de définir une fonction comme étant une subdivision organisationnelle d'un système qui correspond à un ensemble d'opérations orientées vers les mêmes objectifs. Les fonctions peuvent être très variées. Le Tableau 4.4 présente quelques fonctions de même que leur définition.

Tableau 4.4 - Définitions de certaines fonctions.

Fonction	Définition
Production – Transformation	Ensemble des activités qui permettent de créer, à partir d'une ressource utilisée, une nouvelle ressource.
Transport - distribution	Ensemble des activités élémentaires qui permettent de déplacer une ressource.
Stockage	Ensemble des activités qui permettent l'emmagasinement ou la mise en réserve d'une ressource.
Maintenance - Entretien	Ensemble des activités qui permettent de maintenir le système en état de fonctionnement.
Contrôle	Ensemble des activités qui permettent la vérification partielle ou totale de l'état d'un système.
Protection	Ensemble des activités qui permettent de diminuer la vulnérabilité et la dysfonction d'un système.

Le Tableau 4.4 présente des fonctions reliées à l'exploitation d'une infrastructure essentielle. Toutefois, bien d'autres types de fonctions existent. Dans la majorité des cas, ces fonctions correspondent aux cheminées d'affaires ou aux services constituant un système comme les finances ou les ressources humaines.

Une mission nécessite donc la mise en œuvre de fonctions qui utilisent des infrastructures (Figure 4.2).

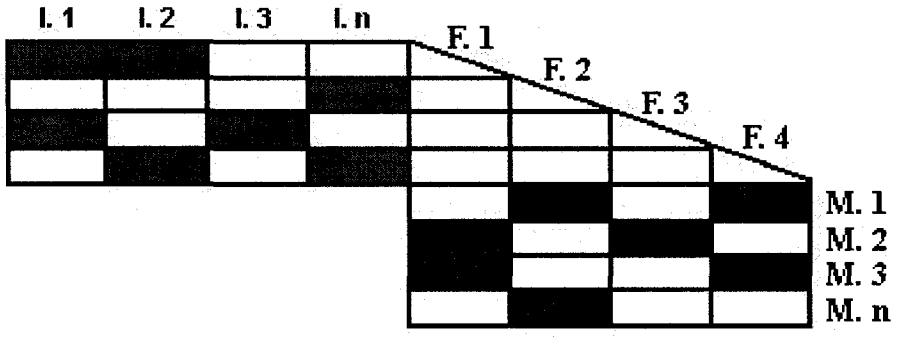

Figure 4.2 - Organisation d'un système.

La Figure 4.2 représente sous forme matricielle le mode d'organisation d'un système. Les cases remplies correspondent à des interactions identifiées entre les composantes du système. La mission 1 (M_1), pour être remplie, nécessite la réalisation des fonctions 2 et 4 (F_2 et F_4). La fonction 2 n'a besoin que de l'infrastructure n pour être réalisée tandis que la fonction 4 a besoin des infrastructures 2 et n. Ce mode de représentation est intéressant, car il permet de visualiser facilement et rapidement l'organisation d'une infrastructure essentielle, mais, surtout, il permet de caractériser l'importance des composantes de cette infrastructure essentielle. En effet, la Figure 4.2 permet de voir quelles infrastructures ou fonctions sont prépondérantes pour le plus grand nombre de missions. Il est évident que l'importance de la mission pour le réseau doit également être considérée.

Pour remplir sa mission, une infrastructure essentielle est donc constituée de fonctions qui vont utiliser des infrastructures. Il est possible de pousser le raffinement plus loin en décomposant les infrastructures en composantes plus petites. Cela dépend du niveau d'analyse et de la précision voulus. Par exemple, nous pouvons considérer une centrale hydroélectrique comme une infrastructure, tel que présenté dans le Tableau 4.3 ou nous pouvons pousser plus loin l'analyse et considérer les infrastructures et les équipements constituant cette centrale. La

Figure 4.3 présente un exemple de raffinement pouvant être effectué pour un aménagement hydroélectrique.

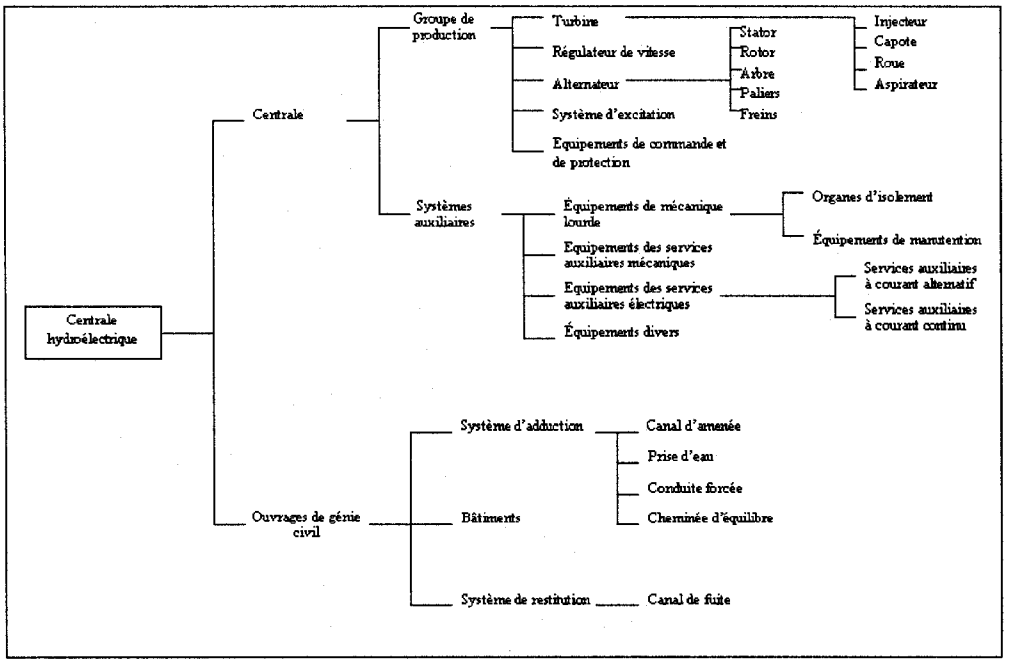

Figure 4.3 - Organigramme technique d'un aménagement hydroélectrique.

Pour obtenir ce genre de diagramme, il faut réaliser une décomposition hiérarchique s'apparentant à un organigramme technique. Il s'agit donc de caractériser par niveaux successifs les composantes constitutives du système étudié. Dans le cas de la Figure 4.3, la centrale hydroélectrique est constituée d'une centrale et d'ouvrages de génie civil. Les ouvrages de génie civil sont le système d'adduction, les bâtiments et le système de restitution. Cet organigramme technique portant sur les infrastructures peut se baser sur les plans de la centrale hydroélectrique.

À l'instar des infrastructures, il est également possible de raffiner les éléments pris en compte pour les fonctions du système en réalisant une analyse fonctionnelle interne. Tel que nous les avons définies, les fonctions peuvent se décomposer en activités qui peuvent elles-mêmes se subdiviser en tâches à réaliser. Tout comme

dans le cas des infrastructures, il s'agit de définir en niveaux successifs les tâches et les activités constitutives d'une fonction donnée. La Figure 4.4 présente un exemple de cette décomposition.

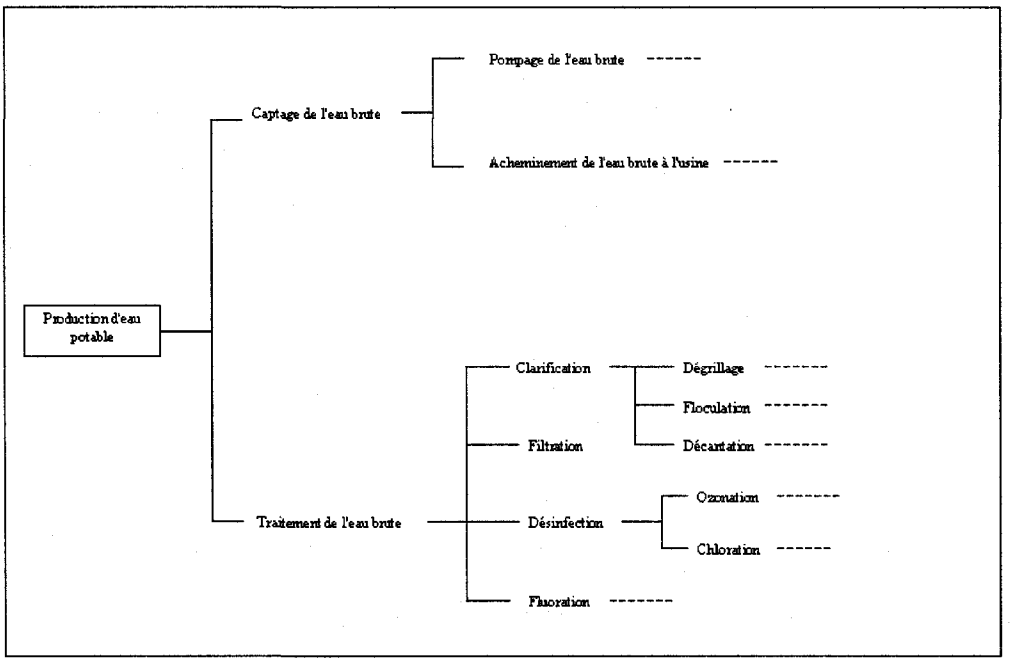

Figure 4.4 - Analyse fonctionnelle de la production d'eau potable.

La Figure 4.4 montre que pour la production d'eau potable, il faut capter de l'eau brute et la traiter. Le traitement implique plusieurs activités (clarification, filtration, désinfection et fluoration). Chacune de ses activités peut être décomposée en tâches spécifiques. Par exemple, la clarification de l'eau brute nécessite du dégrillage, de la floculation et de la décantation.

Le niveau de raffinement de l'organigramme technique ou de l'analyse fonctionnelle dépend directement du contexte et de l'objectif de l'étude. En effet, c'est le responsable de la gestion des risques qui devra décider quel niveau de l'organigramme technique ou de l'analyse fonctionnelle considérer. Cela influera directement sur les actions à prendre pour renforcer le système tant au niveau de ses infrastructures qu'au niveau de ses fonctions.

D'autre part, il est évident que les fonctions et les infrastructures sont reliées puisque les secondes sont mises en place pour permettre la réalisation des premières. Chacune des composantes présentées dans la Figure 4.4 peut-être associée à, au minimum, une infrastructure. Par exemple, le dégrillage nécessite un dégrilleur, mais également une dérivation où pourra s'effectuer un dégrillage manuel.

La création d'un organigramme technique et d'une analyse fonctionnelle apparaît donc importante pour pouvoir caractériser un système et son état. En effet, il est possible de considérer que l'état du système est directement relié à l'état de l'ensemble de ses constituantes que sont les infrastructures et les fonctions.

En fait pour caractériser l'organisation d'un système, il suffit de se poser une série de quatre questions :

- quelles sont les missions du système ?
- quelles sont les fonctions nécessaires pour remplir les missions identifiées ?
- quelles sont les infrastructures nécessaires pour réaliser les fonctions identifiées ?
- quelles sont les ressources nécessaires pour faire fonctionner les infrastructures et réaliser les fonctions du système ?

La définition des missions du système va permettre d'identifier à quels besoins répond le système et donc quelles sont les ressources qu'il fournit.

La réponse à la deuxième question sur les fonctions peut être trouvée avec l'analyse fonctionnelle du système et va permettre d'identifier les fonctions principales dont la variation d'état va affecter la réalisation des missions auxquelles elles sont liées.

La réponse à la troisième question sur les infrastructures peut être trouvée avec l'organigramme technique du système et va permettre d'identifier les

infrastructures principales dont la variation d'état va affecter la réalisation des fonctions auxquelles elles sont liées.

La réponse à la quatrième question se fera en effectuant une analyse fonctionnelle externe. Il faudra pour cela bien identifier les besoins du système à l'étude, mais aussi favoriser les échanges d'information avec les autres systèmes qui fournissent ces ressources.

Les réponses à ces quatre questions vont permettre de caractériser le système de même que ce qui y entre et en sort. La Figure 4.5 montre la caractérisation du système que nous obtenons.

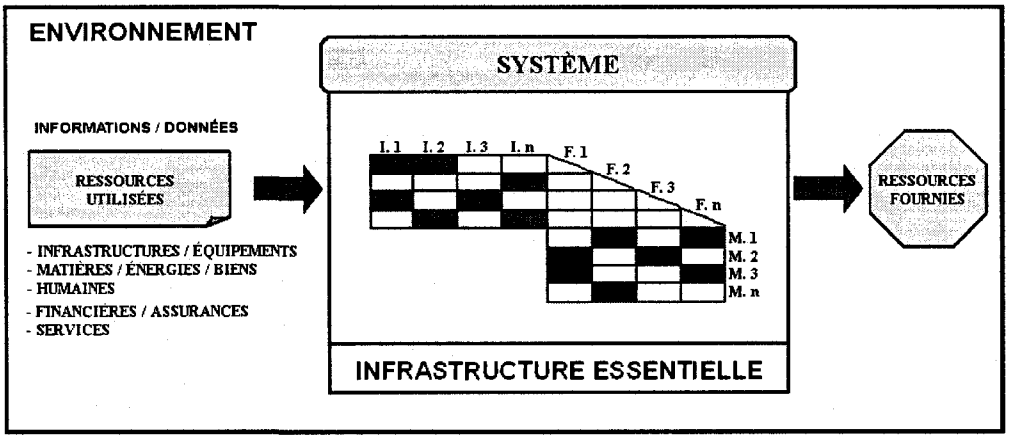

Figure 4.5 - Intégration d'un système dans son environnement.

Pour illustrer le mode d'utilisation de la Figure 4.5, nous pouvons prendre l'exemple d'une infrastructure essentielle de production et de distribution d'eau potable. La ressource fournie par ce système est de l'eau potable. Cette ressource est fournie sur différents secteurs. La mission M_2 de cette infrastructure essentielle correspond à la distribution d'eau potable sur un secteur donné. Pour remplir cette mission, le système utilise deux fonctions, les fonctions F_1 et F_3. La fonction F_1 correspond au transport de l'eau tandis que la fonction F_3 correspond au stockage de l'eau. Pour assurer ces deux fonctions, le système utilise trois infrastructures, les

infrastructures I_1, I_2 et I_3. L'infrastructure I_1 est un centre de contrôle permettant d'opérer certaines parties du système. Cette infrastructure particulière est utilisée pour réaliser les fonctions F_1 et F_3. L'infrastructure I_2 est une conduite primaire. Cette infrastructure est nécessaire pour la réalisation de la fonction F_1. L'infrastructure I_3 est un réservoir de stockage qui sert spécifiquement pour la réalisation de la fonction F_3.

La Figure 4.5 permet également de voir que le système utilise des ressources (ressources utilisées) pour fonctionner. Parmi celles-ci, nous pouvons noter les informations et données qui vont notamment être nécessaires pour les opérations de l'infrastructure de contrôle du système (I_1) et par conséquent pour la réalisation des fonctions F_1 et F_3 et de la mission M_2.

L'organisation du système ainsi caractérisée permet de considérer l'ensemble des éléments constitutifs du risque comme le montre le Tableau 4.5.

Tableau 4.5 - Éléments constitutifs du risque pour une infrastructure essentielle.

Composantes du risque	Élément correspondant pour une infrastructure essentielle
Aléas	Dégradation d'une ressource utilisée.
Vulnérabilité	Affectation des fonctions, des infrastructures ou de la mission du système.
État	État des fonctions ou des infrastructures composant le système. État des ressources fournies et utilisées.
Dysfonction	Dégradation de l'état de la mission du système.
Conséquences	Dégradation de la ressource fournie.
Effet domino	Affectation d'un autre système.

Les éléments que nous proposons semblent bien s'articuler d'un point de vue théorique. Il faut tout de même voir s'ils sont applicables de manière pratique.

4.3 Application des concepts proposés

L'utilisation des organigrammes techniques et des analyses fonctionnelles est relativement répandue dans le domaine industriel. Ces outils sont à la base même de la gestion de projet. En effet, un organigramme technique permet de définir le contenu ou la portée d'un projet tandis que l'analyse fonctionnelle est une méthode utilisée pour caractériser les fonctions d'un système en vue de répondre de façon optimale à un besoin précis (Tassinari, 2003 ; Project Management Institute, 2008). Dans le contexte plus spécifique de la gestion des risques, les analyses fonctionnelles sont à la base de certaines méthodes d'analyse utilisées dans le domaine de la sûreté de fonctionnement, telles que les méthodes AMDEC et HAZOP (Garin, 1994 ; Modarres et coll., 1999). L'originalité ne repose donc pas dans l'utilisation de ces outils, mais bien dans l'utilisation que nous proposons d'en faire. Le premier élément est que nous préconisons l'utilisation de ces outils pour des systèmes existants alors qu'à la base ils sont généralement employés pour des systèmes qui sont à un stade de développement. De plus, nous proposons de combiner ces deux outils pour identifier les infrastructures et fonctions importantes d'un système ce qui n'est pas forcément leur objectif premier.

En fait, l'originalité de l'utilisation de l'analyse fonctionnelle et de l'organigramme technique tient à deux éléments :

1. le fait que nous proposons d'utiliser ces techniques alors que nous ne sommes plus à un niveau de gestion de projet ;
2. le fait que nous proposons de combiner ces techniques pour caractériser un système en termes de missions, fonctions et infrastructures nécessaires pour son bon fonctionnement.

Nous avons pu vérifier cette possibilité de décomposer un système en missions, fonctions et infrastructures par une application réalisée pour le système de

production d'eau potable de la ville de Montréal. Pour cette étude, nous avons analysé l'ensemble d'une usine de production d'eau potable. Nous posons donc les questions que nous avons identifiées comme permettant de soutenir notre analyse.
Quelles sont les missions du système ?
L'usine de production d'eau potable a deux missions principales qui sont de produire de l'eau potable et de fournir un certain volume d'eau à la ville de Montréal.

Quelles sont les fonctions nécessaires pour remplir les missions identifiées ?
Nous répondons à cette question en réalisant une analyse fonctionnelle interne de l'usine d'eau potable et donc en représentant sous forme arborescente l'ensemble des activités nécessaires à la production d'eau potable.

Quelles sont les infrastructures nécessaires pour réaliser les fonctions identifiées ?
Nous répondons à cette question en réalisant un organigramme technique de l'usine d'eau potable et donc en représentant sous forme arborescente l'ensemble des équipements nécessaires aux différentes fonctions permettant de produire de l'eau potable

La Figure 4.6 présente une combinaison d'une partie de l'analyse fonctionnelle et de l'organigramme technique réalisés.

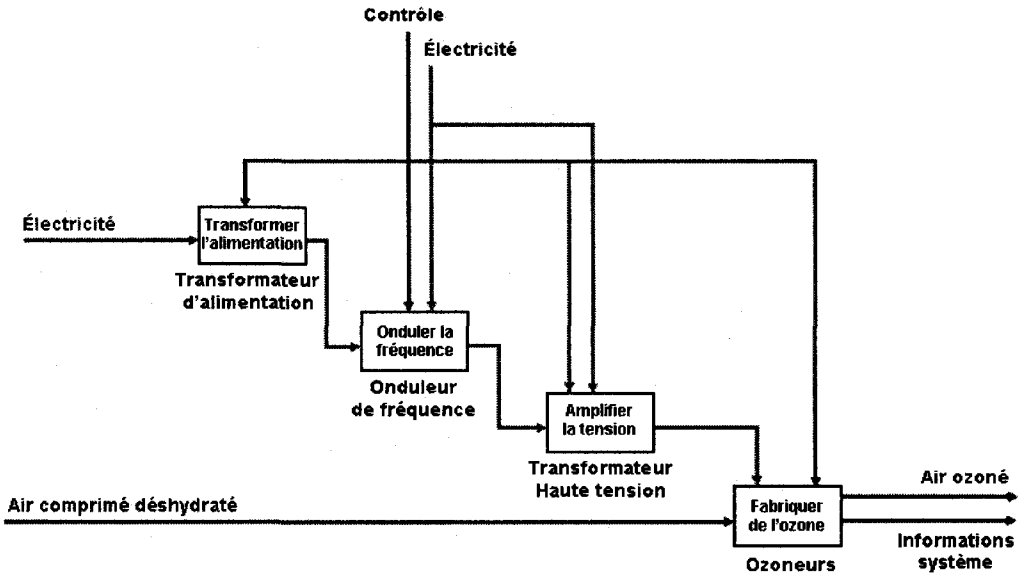

Figure 4.6 - Analyse fonctionnelle et organigramme technique de la production d'ozone (Guillaume, 2005)

La Figure 4.6 détaille les opérations à effectuer de même que les équipements nécessaires pour la fonction de production de l'ozone qui sert pour la désinfection de l'eau. Pour produire de l'ozone, il faut donc principalement modifier la tension de la ressource électrique de manière à pouvoir alimenter les ozoneurs qui vont permettre de produire de l'ozone à partir d'air comprimé préalablement déshydraté.

Le même type d'analyse est effectué pour l'ensemble du système « usine d'eau potable ». Cela permet d'identifier les composantes les plus importantes pour le fonctionnement du système de même que les ressources qu'elles utilisent et qu'elles fournissent.

Ce mode d'analyse permet donc d'introduire un autre élément novateur de nos travaux : la considération de tout système comme étant une entité utilisatrice et fournisseuse de ressources. Cette manière de considérer les systèmes permet de répondre à notre quatrième question à savoir quelles sont les ressources nécessaires pour faire fonctionner les infrastructures et réaliser les fonctions du système.

La réponse à cette question permet de considérer les interdépendances entre systèmes, mais également de mieux définir les niveaux de conséquences pouvant être engendrés pour l'environnement du système. Cette manière de considérer un système dans son environnement est largement employée dans l'ensemble des travaux de recherche effectués par le *Centre risque & performance* (Robert et Morabito, 2009).

Dans l'exemple présenté à la Figure 4.6, nous voyons que le système utilise deux ressources, de l'électricité et de l'air comprimé déshydraté. L'exemple présenté montre également que la partie du système analysé permet de produire deux ressources utilisées à l'interne que sont des données pour le contrôle du système et de l'ozone pour le traitement de l'eau.

Il est intéressant de constater que quelle que soit l'échelle à laquelle se fait l'analyse le concept d'entité utilisant et fournissant des ressources est toujours valable. En effet, de la manière la plus commune, une infrastructure essentielle est considérée comme une entité fournissant et utilisant des ressources. Toutefois, si nous analysons une infrastructure essentielle en détail, chacune de ses composantes (infrastructures et fonctions) peut être considérée comme une entité qui fournit et utilise des ressources.

4.4 Conclusion

L'organisation d'un système est particulièrement importante dans un contexte de gestion des risques. En effet, elle permet de caractériser l'état d'un système, état qui est à la base même de la notion de risque.

Ce chapitre a permis de montrer le mode d'organisation d'un système et comment il est possible d'analyser cette organisation. Pour cela, nous avons présenté à la fois notre approche de manière théorique et à la fois de manière pratique en utilisant un exemple d'application réalisée pour l'usine de production d'eau potable de la ville de Montréal. Notre approche montre que l'utilisation d'une succession de questions

simples permet de poser les bases d'une analyse de l'organisation d'un système complexe. Elles sont présentées ci-après.

1. Quelles sont les missions du système ?
   La réponse à cette question permet d'identifier les ressources fournies par le système étudié. Elle peut être obtenue en réalisant une analyse fonctionnelle externe.

2. Quelles sont les fonctions nécessaires pour remplir les missions identifiées ?
   La réponse à cette question permet d'identifier les fonctions importantes du système étudié. Elle peut être obtenue en réalisant une analyse fonctionnelle interne.

3. Quelles sont les infrastructures nécessaires pour réaliser les fonctions identifiées ?
   La réponse à cette question permet d'identifier les infrastructures importantes du système étudié. Elle peut être obtenue en réalisant un organigramme technique.

4. Quelles sont les ressources nécessaires pour faire fonctionner les infrastructures et réaliser les fonctions du système ?
   La réponse à cette question permet d'identifier les ressources utilisées par le système étudié. Elle peut être obtenue en réalisant une analyse fonctionnelle externe.

Ce chapitre a donc permis d'atteindre en partie le deuxième objectif de ce travail qui était de caractériser les différents groupes de fonctions constitutives d'une infrastructure essentielle. Cela permet de vérifier la deuxième hypothèse sous-

tendant cette recherche à savoir qu'un système peut être défini en fonction de ses missions, fonctions et besoins.

De plus, ce chapitre permet également de conforter notre première hypothèse de travail à savoir que le concept de vulnérabilité et la notion d'état d'un système sont des composantes intrinsèques du risque. En effet, la caractérisation du système permet de faire ressortir les six éléments qui sont constitutifs du risque tel que défini dans le chapitre précédent.

CHAPITRE 5 MÉTHODOLOGIE D'ANALYSE DES VULNÉRABILITÉS

Nous avons vu dans les chapitres précédents que le risque peut être défini comme la combinaison de six éléments :

- les aléas ;
- les vulnérabilités du système ;
- l'état du système ;
- les dysfonctions du système ;
- les conséquences ;
- les effets domino.

En appliquant cette définition du risque à la problématique des infrastructures essentielles, nous avons montré que chacune de ces composantes du risque pouvait être retrouvée dans le cadre de la caractérisation d'une infrastructure essentielle (chapitre 4).

Comme l'a montré le chapitre 3 sur la définition du risque, beaucoup de travaux font appel à la notion de vulnérabilité. Cette tendance se reflète également pour la gestion des risques associée aux infrastructures essentielles. En effet, les travaux du Groupe de planification nationale des contingences (GPNC) étaient directement reliés à cette notion de vulnérabilité (GPNC, 2000). Les travaux de l'Argonne national laboratory font également référence à cette notion de vulnérabilité des infrastructures essentielles face à leurs dépendances à d'autres infrastructures essentielles (Peerenboom and Fisher, 2007).

Nous avons également vu dans le chapitre sur le risque que cette notion de vulnérabilité pouvait s'appliquer à de nombreux éléments de natures différentes et pouvait être complexe à définir.

Une autre problématique importante qui nous intéresse plus particulièrement est la prise en compte et l'intégration de la cybernétique dans l'analyse et l'évaluation

des vulnérabilités des infrastructures essentielles. Il s'agit de définir ce qu'est exactement la cybernétique et de définir comment intégrer ses spécificités dans une méthodologie d'analyse des vulnérabilités.

Dans ce chapitre, nous allons faire le point sur l'analyse de vulnérabilité et faire ressortir les éléments importants, mais aussi les faiblesses des approches actuelles.

Nous présenterons également l'approche que nous proposons pour pouvoir effectuer l'analyse de vulnérabilité d'une infrastructure essentielle en considérant plus spécifiquement la dépendance face à la cybernétique.

5.1 Analyse de vulnérabilité : Problématique

Comme nous l'avons montré dans le chapitre 3, la notion de vulnérabilité est directement liée à l'état du système étudié, mais également aux aléas tant internes qu'externes qui pourraient l'affecter.

De manière générale, les analyses effectuées pour les infrastructures essentielles et, plus globalement, au niveau industriel, portent sur le risque sans vraiment considérer l'état du système. L'utilisation des scénarios normalisés et alternatifs en est un bon exemple (CRAIM, 2007). Dans la majorité des cas, les scénarios sont conçus en début de projet et en considérant un fonctionnement optimal des composantes du système, tout du moins en ce qui concerne les mesures de protection. La vulnérabilité du système, bien que sous-jacente, n'est pas vraiment considérée. Ces méthodes ont comme point de départ la défaillance du système liée à un aléa. Ces méthodes ne permettent pas de définir l'ensemble des vulnérabilités du système.

Les méthodes de sûreté de fonctionnement (Arbres, AMDEC, HAZOP, MADS-MOZAR, etc.), bien qu'analysant le risque, s'attardent un peu plus sur la vulnérabilité du système (Garin, 1994 ; INERIS, 2003). En effet, le but de ces méthodes est de se prémunir face à un aléa en mettant en œuvre des mesures de

protection ou d'atténuation. Cependant, tout comme dans le cas des méthodes de scénarios normalisés ou alternatifs, ces méthodes ne semblent pas véritablement considérer l'état du système à l'étude et la variation de cet état.

Les méthodes de sûreté de fonctionnement présentent des avantages et des inconvénients. Ces points positifs et négatifs devront être considérés dans l'élaboration de notre méthodologie d'analyse des vulnérabilités d'une infrastructure essentielle.

Si nous considérons plus spécifiquement la méthode d'analyse des modes de défaillance, de leurs effets et de la criticité (AMDEC), il est possible de faire ressortir les avantages suivants :

- elle se base sur une analyse fonctionnelle interne du système ;
- elle permet de déterminer un indicateur de niveau de risque, la criticité, qui correspond à une combinaison d'indicateurs portant sur le potentiel de détection d'une défaillance, sa possibilité d'occurrence et finalement sur le niveau de sévérité des conséquences pouvant être engendrées ;
- le mode de représentation des résultats sous forme de tableaux facilite la prise de décision et l'intervention sur le système.

Cependant, la méthode AMDEC présente également les inconvénients suivants :

- AMDEC est une approche inductive et, en ce sens, elle contribue plus à une gestion réactive du risque qu'à une gestion proactive ;
- le mode de calcul de la criticité est discutable. L'intégration de l'importance des composantes pour le fonctionnement du système serait intéressante ;
- elle n'intègre pas véritablement les conséquences de la défaillance du système de même que ses dépendances face à son environnement ;
- les aléas considérés sont principalement des aléas techniques internes ;
- son application peut s'avérer longue et difficile dans le cas de système complexe comme les infrastructures essentielles.

L'organisation de la méthode AMDEC de même que le mode de représentation sous forme de tableau montre que cette méthode est véritablement centrée sur le système et sa protection. Ceci s'explique puisque cette méthode est une méthode servant principalement à la conception de systèmes industriels.

Dans notre cas, le système et son état sont prépondérants. Toutefois, il apparaît important d'axer également notre analyse sur les interfaces du système avec son environnement en considérant ses vulnérabilités et ses dysfonctions.

Dans la prochaine section, nous allons présenter la méthodologie que nous proposons.

5.2 Méthodologie d'analyse des vulnérabilités d'une infrastructure essentielle

Les principes de sûreté de fonctionnement à la base de la méthode AMDEC servent de base au développement d'une méthodologie adaptée à notre problématique à savoir l'analyse des vulnérabilités d'une infrastructure essentielle.

Nous avons vu dans le chapitre précédent que les éléments que nous devons considérer sont :

- les ressources utilisées par le système dont les données et les informations. Ce sont les aléas.
- l'état du système et de ses composantes (infrastructures, fonctions, missions).
- les ressources fournies par le système. Ce sont les conséquences.

La Figure 5.1 montre le mode d'organisation de ces éléments.

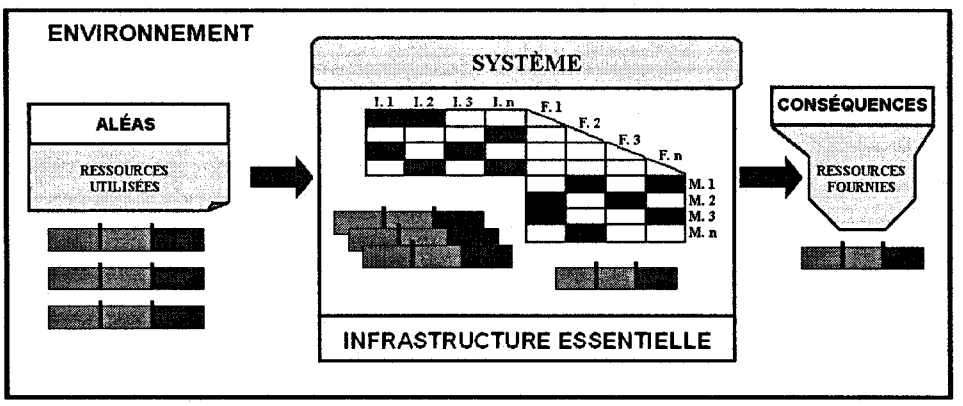

Figure 5.1 – Triplet Aléas – Système - Conséquences.

Le premier élément important est l'environnement qui englobe l'ensemble des éléments à considérer. En effet, le système utilise des ressources qui proviennent de cet environnement et il fournit d'autres ressources à ce même environnement. De ce fait, l'analyse d'un système ne peut se faire indépendamment de l'environnement dans lequel il s'intègre.

Le deuxième élément important est le système. Ce système peut être de natures diverses (industries, infrastructures essentielles, etc.). Quelle que soit sa nature, tout système peut être caractérisé de la même façon. Un système sert à transformer ou déplacer des ressources. Pour cela, il est constitué de fonctions et d'infrastructures qui lui permettent de remplir sa ou ses missions. La Figure 5.1 présente le mode d'organisation d'un système. Cette figure indique que la mission 2 du système (notée M.2) nécessite la réalisation des fonctions 1 et 3 du système (notées respectivement F.1 et F.3). La fonction 1 (notée F.1) quant à elle utilise les infrastructures 1 et 2 du système (notées respectivement I.1 et I.2). Une chose importante à noter est que les fonctions et les infrastructures du système nécessitent l'utilisation de ressources.

En effet, dans un déroulement temporel, une ressource est utilisée par le système pour pouvoir remplir sa mission qui correspond à la fourniture d'une nouvelle ressource. Le risque se matérialise lorsque la ressource utilisée ou une composante

du système va mal fonctionner ce qui va entraîner une dégradation de la ressource fournie.

Il est possible d'analyser le problème de manière inductive soit dans le sens du déroulement temporel des événements. En partant d'un aléa interne ou externe, il faut alors analyser la réaction du système et la répercussion sur son environnement. C'est cette approche qui est généralement privilégiée avec la détermination de scénarios considérant des aléas extrêmes.

Cependant, il apparaît plus intéressant dans un objectif de planification des mesures d'urgence et de continuité opérationnelle d'aborder l'analyse de manière déductive en partant de l'objectif du système soit la fourniture de ressources et d'analyser les besoins pour réaliser cet objectif. En effet, de cette manière, nous nous intéressons véritablement au mode de fonctionnement du système et cela permet d'identifier ses composantes les plus importantes, mais également les mesures de protection ou d'atténuation qui pourraient être mises en place pour renforcer le système. De plus, cette approche permet plus facilement de s'intéresser à la vulnérabilité du système face aux ressources qu'il utilise.

La méthodologie d'analyse des vulnérabilités d'un système que nous proposons est donc une méthode déductive c'est-à-dire qu'elle part de l'analyse des conséquences sur l'environnement résultant des dysfonctions du système pour finir par l'analyse des aléas pouvant être à leur origine. Elle se subdivise en quatre étapes (Figure 5.2) :

1. caractérisation de l'environnement du système ;
2. caractérisation du système ;
3. caractérisation des besoins du système ;
4. amélioration continue.

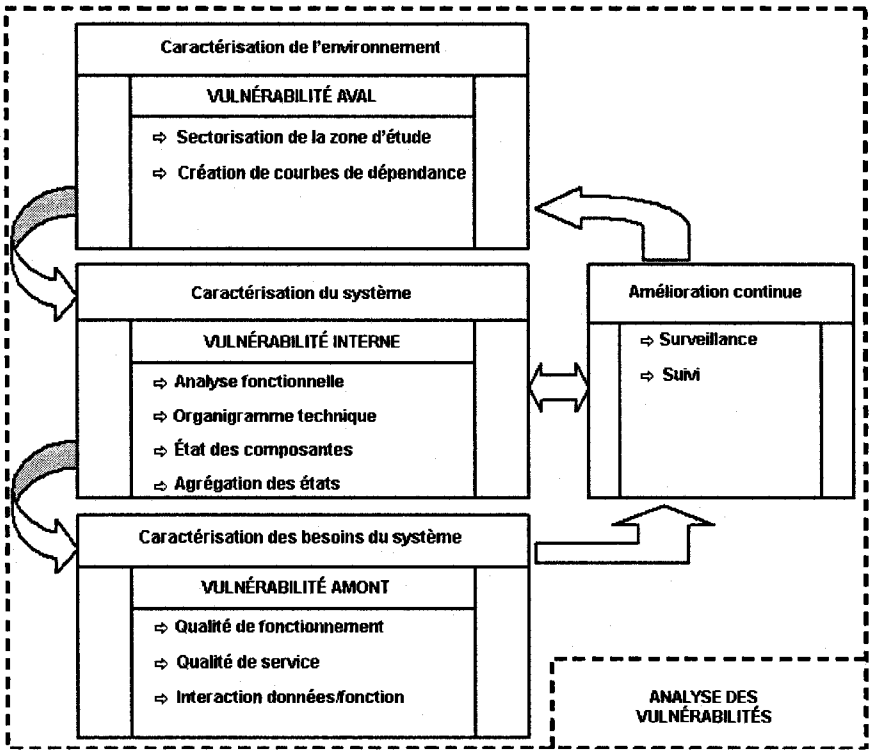

Figure 5.2 - Les différentes étapes de la méthodologie d'analyse des vulnérabilités.

Cette manière de procéder permet d'analyser la vulnérabilité à différents niveaux. En effet, pour chaque étape, il est possible de caractériser une vulnérabilité particulière. Un peu comme dans le cas de la définition de la vulnérabilité de Blancher (1998), il est possible de caractériser une vulnérabilité aval (correspondant aux conséquences sur l'environnement), une vulnérabilité interne (correspondant à l'état du système) et une vulnérabilité amont (correspondant aux dépendances du système face à ses besoins). Il s'agit en fait de déterminer les points faibles ou les éléments sensibles qui pourraient contribuer à la matérialisation d'une des composantes du risque. C'est à l'étape de la caractérisation des besoins du système qu'est plus particulièrement prise en compte la cybernétique par l'entremise de l'analyse de la dépendance du système face à l'utilisation de données.

Dans les parties suivantes de ce chapitre, nous allons voir chacune des étapes de caractérisation de même que l'étape d'amélioration continue que nous proposons dans notre méthodologie d'analyse des vulnérabilités d'une infrastructure essentielle.

5.2.1 Caractérisation de l'environnement du système

La caractérisation de l'environnement du système permet d'analyser la vulnérabilité aval c'est-à-dire d'analyser l'effet des ressources fournies par le système sur son environnement. La caractérisation de l'environnement est donc une étape déterminante dans la caractérisation des interdépendances entre infrastructures essentielles. Pour cela, il faut segmenter l'environnement en secteurs différents. Cette manière de procéder permet en effet de développer des actions plus efficaces en termes de mesures d'urgence, mais aussi de soutenir adéquatement la mise en œuvre d'un système d'alerte précoce.

La détermination de la vulnérabilité aval n'est pas véritablement l'objet de cette thèse. Le mode de caractérisation de l'environnement ne sera donc présenté que de manière générale. Il semble important de le présenter dans le sens ou ce travail de doctorat a permis de poser les principes de cette caractérisation. La présentation des principes de cette caractérisation de l'environnement du système permettra aux lecteurs d'avoir une vision globale de la démarche développée au *Centre risque & performance* dans laquelle s'intègre ces travaux.

Plusieurs solutions s'offrent pour segmenter l'environnement. La première consiste à utiliser les caractéristiques urbanistiques en se servant des axes routiers pour délimiter des zones. Cette approche est relativement simple et présente l'avantage de pouvoir s'effectuer à partir d'une carte topographique et de pouvoir être géoréférencée. Cependant, elle présente un inconvénient. Les secteurs ainsi définis ne sont pas forcément adaptés à la réalité de fonctionnement des systèmes, mais surtout des caractéristiques physiques de l'environnement. Il est sans doute possible de raffiner ce mode de sectorisation en intégrant les caractéristiques de

l'environnement et des systèmes considérés. Toutefois, le problème de la confidentialité des données se pose alors. Les gestionnaires de système sont en effet très réticents à donner les localisations précises de leurs équipements et infrastructures en raison des problèmes de sécurité que cela pourrait engendrer.

Une façon de résoudre ce problème est de sectoriser la zone d'étude (environnement) de manière arbitraire en délimitant des secteurs de même surface. C'est ce que Robert et Morabito (2008) qualifient de cartographie souple. La Figure 5.3 présente un exemple de ce mode de sectorisation appliquée pour le centre-ville de la ville de Montréal au Québec.

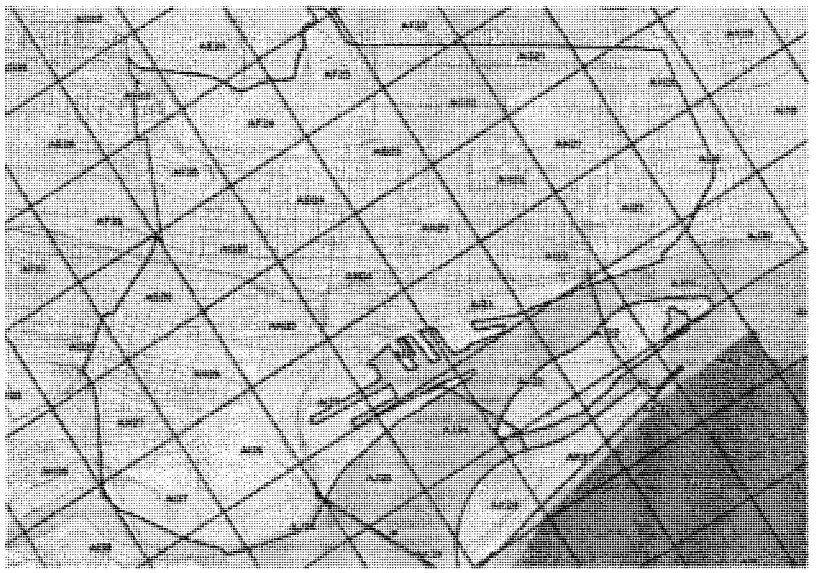

Figure 5.3 - Cartographie souple appliquée à la ville de Montréal (Robert and Morabito, 2008)

A priori, il n'y a rien d'extraordinaire dans cette division d'une zone d'étude en carrés. Effectivement, cette manière de faire facilite l'échange d'information entre les différents acteurs des mesures d'urgence (utilisation de numéro pour chaque carré). Elle permet également une localisation géographique plus précise (carrés orientés suivant le nord). Toutefois, l'avantage principal de ce mode de sectorisation est l'utilisation qui peut en être faite. En effet, les gestionnaires

d'infrastructures essentielles peuvent localiser leurs équipements et infrastructures en étant libres de la précision qu'ils veulent utiliser. Ils peuvent préciser dans quels carré ou groupes de carrés se trouvent les équipements constituant leurs réseaux. Cette latitude leur permet de gérer un niveau de vulnérabilité acceptable en termes d'actes de malveillance face à la localisation de leurs infrastructures. Plus la localisation est précise, plus l'information est pertinente pour être utilisée dans un processus de gestion des risques.

De manière à caractériser de façon optimale l'environnement, d'autres critères peuvent être utilisés. Il est évident que le nombre de critères permettant de caractériser la zone d'étude dépend de l'objectif de l'analyse, du niveau de raffinement recherché, mais également du type de conséquences caractérisé.

En se focalisant principalement sur les interdépendances entre infrastructures essentielles, les critères de sectorisation et de caractérisation de l'environnement du système vont essentiellement dépendre du type de lien de dépendance considéré :

- physique ;

  Un lien physique est une relation de dépendance physique existant entre deux infrastructures essentielles. Ces liens sont mis en place volontairement pour permettre le fonctionnement des infrastructures essentielles. Les conduites, les câbles et les rails de chemin de fer sont des exemples de liens physiques.
- géographique ;

  Un lien géographique est une relation de dépendance existant entre deux infrastructures essentielles en raison de leur localisation géographique, de l'utilisation de corridors communs. Ces liens se matérialisent lors de la défaillance d'une infrastructure essentielle. La fuite d'une conduite d'eau, qui pourrait avoir des effets sur des conduites de gaz situées à proximité de la conduite d'eau, est un exemple de lien géographique.
- Logique ;

  Un lien logique est une relation de dépendance entre deux infrastructures essentielles qui est reliée aux règles de fonctionnement d'une des

infrastructures. Les législations, les règlements, les décisions humaines et le domaine de la finance sont des exemples de liens logiques.

- cybernétique ;
  Un lien cybernétique est une relation de dépendance entre deux infrastructures essentielles dédiée à la transmission de données et d'informations par le biais de procédés électromagnétiques, ondulaires ou informatiques. Ces liens sont créés volontairement. Le réseau Internet et les systèmes de contrôle à distance sont des exemples de liens cybernétiques.

Pour caractériser les interdépendances physiques entre infrastructures essentielles, trois critères de sectorisation sont nécessaires :

- la caractérisation des secteurs de fourniture de la ressource fournie par le système étudié ;
- la caractérisation des infrastructures essentielles présentes dans les secteurs définis ;
- la caractérisation des relations de dépendance entre le système et les infrastructures essentielles présentes dans l'environnement.

La caractérisation des secteurs de fourniture du système permet de déterminer le secteur d'affectation de la ressource fournie par le système évalué. Pour cela, il faut diviser la zone d'étude (environnement) en secteurs ayant des caractéristiques similaires en termes de fourniture de ressources. En effet, c'est la dégradation de l'état de la ressource ou des ressources fournies par un système (dysfonction du système) qui va potentiellement engendrer des conséquences sur l'environnement. Il faut donc nécessairement connaître où vont se faire ressentir ces dysfonctions. Pour cela, la connaissance des secteurs de fourniture des ressources semble la meilleure solution.

La caractérisation des infrastructures essentielles permet de déterminer les éléments importants présents dans l'environnement du système qui pourraient utiliser la ressource fournie par l'infrastructure essentielle analysée. Il s'agit donc de définir

les éléments valorisés de l'environnement qui se trouvent dans les secteurs définis et donc dans la sphère d'influence du système. Les éléments valorisés de l'environnement regroupent tous les éléments qui peuvent avoir une importance particulière pour les objectifs de l'analyse (André et coll., 2003). Il est évident que les éléments importants dans le cadre de la caractérisation des interdépendances entre infrastructures essentielles sont les infrastructurelles essentielles elles-mêmes. Plus la localisation de ces éléments sera précise, plus l'analyse et l'évaluation le seront. Cependant, comme nous l'avons déjà mentionné, une localisation géographique précise peut être difficile à obtenir car elle induit inévitablement un autre niveau de vulnérabilité.

La caractérisation des relations de dépendance entre le système et les infrastructures essentielles présentes dans l'environnement permet de générer des courbes de dépendance qui sont particulièrement utiles en termes de continuité opérationnelle et de mesures d'urgence. En effet, ces courbes permettent de visualiser la variation d'état de la fourniture d'une ressource donnée en fonction de l'utilisation qui en sera fait.

La Figure 5.4 montre un exemple de courbe de dépendance qui peut être obtenue pour l'utilisation de la ressource électrique par un réseau de distribution d'eau potable. Cet exemple est fictif et a vocation d'illustration de notre propos.

Cette courbe est obtenue en considérant le fonctionnement de pompes utilisées par un réseau de distribution d'eau potable. Le fonctionnement des pompes nécessite une tension de 400 volts. Si le réseau d'électricité ne peut pas lui fournir cette tension, il ne peut donc pas remplir sa mission. Sachant que la tolérance des pompes face à la variation de tension est de 10%, nous obtenons la Figure 5.4.

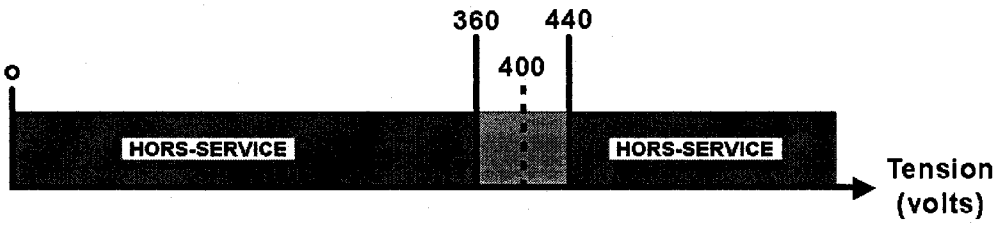

Figure 5.4 - Variation d'état du réseau de distribution d'eau potable.

En considérant la ressource électricité, deux états du réseau d'eau potable peuvent être définis :

- un état normal ou optimal de fonctionnement entre 360 et 440 volts. En effet, pour ce niveau de tension, la fourniture d'électricité n'affectera pas le fonctionnement du réseau d'eau.
- un état hors-service entre 0 et 360 volts et pour une tension supérieure à 440 volts. Pour ces tensions, les pompes doivent être arrêtées entrainant l'arrêt de fonctionnement du réseau d'eau. Le réseau de fourniture d'électricité ne respecte plus les caractéristiques nécessaires au fonctionnement du réseau d'eau potable. Il est donc possible de dire qu'il ne remplit plus sa mission.

En cas d'arrêt total de l'alimentation en électricité ou en cas d'état hors-service de la ressource électricité, le réseau de distribution d'eau potable pourra mettre en œuvre ses mesures de protection. Il pourra en effet mettre en fonctionnement ses génératrices. Elles ont une autonomie de 24 heures. Il est donc possible de créer une nouvelle courbe de dépendance intégrant à la fois la dysfonction du système (électricité) et la dépendance du réseau d'eau face à la ressource alternative essence (Figure 5.5).

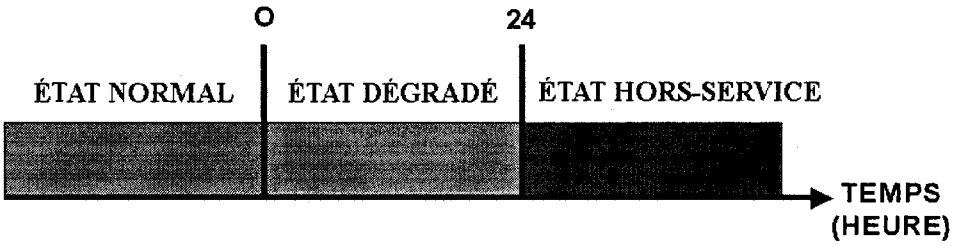

Figure 5.5 - Variation d'état du réseau d'eau.

Cette nouvelle courbe de dépendance intègre un nouveau paramètre de mesure, le temps. En effet, en partant du fait que le système est hors-service, le réseau d'eau qui est dépendant du système doit mettre en œuvre ses mesures d'urgence. Il produit donc de l'électricité à partir de sa génératrice.

Le temps 0 correspond à la mise hors service du système (électricité). Avant cela, le réseau d'eau était dans un état normal. Une fois le système de production d'électricité hors service, le réseau d'eau entre en mesures d'urgence en utilisant ses génératrices. Son état est dégradé durant 24 heures ce qui correspond à l'autonomie des génératrices avant leur mise hors service. L'état du réseau d'eau est dégradé, car il n'est pas en fonctionnement optimal. Un autre aléa affectant les génératrices pourrait provoquer leur arrêt. Si d'autres mesures sont disponibles pour protéger le réseau d'eau ou pour augmenter l'autonomie des génératrices, telles que des mesures de stockage ou d'approvisionnement en essence, elles doivent être intégrées. En effet, elles influeront directement sur le délai ou la marge de manœuvre à la disposition du gestionnaire du réseau d'eau avant que son réseau tombe hors service. Cette information est très importante également pour le gestionnaire du système (réseau électrique). En effet, la Figure 5.5 indique à ce gestionnaire qu'il dispose de 24 heures pour rétablir son système et réalimenter le réseau d'eau.

De plus, cette courbe de dépendance, intégrant le facteur temporel, est très intéressante, car elle permet de poser les bases de discussion et d'échange entre les

gestionnaires des deux infrastructures essentielles. En effet, l'élément temps est prépondérant pour la phase d'intervention. En ayant plusieurs courbes de dépendance, il est possible de mettre en place une priorisation du rétablissement en fonction des conséquences anticipées pour les réseaux dépendants. Ces courbes peuvent permettre également de modifier les paramètres d'opération des différentes infrastructures essentielles en faisant ressortir les niveaux de sensibilité (vulnérabilité aval) des infrastructures essentielles d'un environnement donné.

Il est entre autres possible de développer des courbes de dépendances permettant de caractériser les défaillances en cascades (effets domino) pouvant être générées suite à la défaillance de fonctionnement d'une infrastructure essentielle. La Figure 5.6 présente un exemple d'une courbe de dépendance réalisée pour le centre-ville de Montréal.

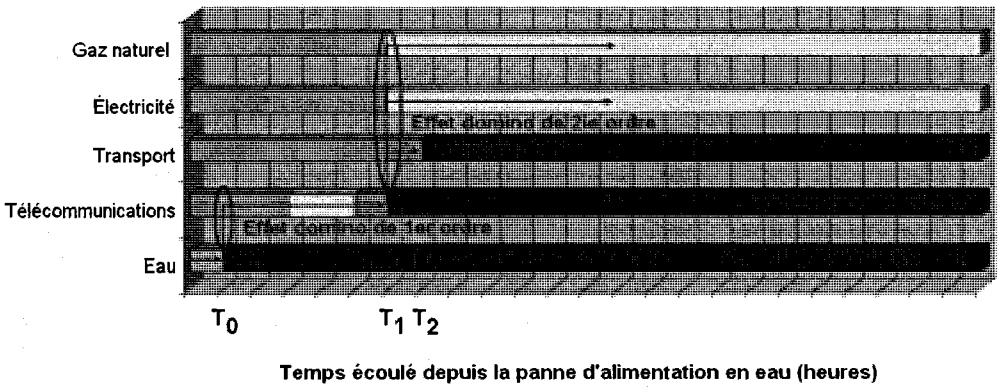

Figure 5.6 - Effets domino engendrés suite à une panne d'alimentation en eau (Robert and Morabito, 2008)

La Figure 5.6 montre qu'une perte d'alimentation en eau, au temps T_0 se traduirait par des répercussions majeures sur les réseaux de télécommunications et de transport. Au temps T_1, l'ensemble de la zone d'étude serait affecté en raison de la perte de service du réseau de télécommunications. Cette perte des télécommunications va se répercuter sur le réseau de transport en engendrant, au temps T_2, la fermeture d'un axe routier situé sur un des secteurs de la zone d'étude. Cette courbe permet donc également de visualiser une interdépendance

cybernétique entre le réseau de télécommunication et le réseau de transport. En effet, le réseau de transport a besoin de données fournies ou acheminées par le réseau de télécommunication.

La caractérisation de l'environnement du système peut utiliser d'autres critères que ceux définis pour caractériser les interdépendances physiques entre infrastructures essentielles. En effet, divers éléments peuvent influer sur les dépendances et les interdépendances entre infrastructures essentielles en considérant les trois autres types de lien (géographique, cybernétique et logique).

Les dépendances découlant des liens géographiques se basent sur les caractéristiques physiques de la ressource et de l'environnement. En ce sens, ces caractéristiques physiques peuvent être considérées dans le mode de sectorisation et dans la caractérisation de l'environnement du système.

Par exemple, pour les ressources liquides (eau, essence, etc.), il faut considérer les éléments pouvant influencer l'écoulement ou la stagnation, telle que la topographie de l'environnement, les systèmes de captage (égouts) pouvant être présents, les zones favorisant l'infiltration, etc. Il faut également prendre en compte les zones d'alimentation des différentes infrastructures essentielles.

Les dépendances découlant des liens logiques ou cybernétiques nécessitent également d'autres critères de sectorisation. En effet, ces liens sont particuliers dans le sens où ils intègrent à la fois des transferts de données et des moyens physiques de communication.

La caractérisation de l'environnement intégrant les interdépendances logiques doit prendre en considération les critères permettant de caractériser le paramètre économique. Il est possible de penser à des éléments intégrant la dépendance des infrastructures essentielles à certaines institutions bancaires ou à certains éléments caractérisant les marchés financiers sur un secteur donné.

La caractérisation de l'environnement intégrant les interdépendances cybernétiques doit prendre en considération la dépendance des infrastructures essentielles aux données et aux informations. Il faut donc intégrer des critères permettant de considérer l'utilisation des données par les infrastructures essentielles, mais également les dégradations possibles de ces données. Il faut donc considérer les données ou les informations comme étant des ressources particulières permettant de faire fonctionner des infrastructures essentielles. Un des critères prépondérants à ce sujet est la notion de délai durant lequel l'infrastructure essentielle peut se passer d'une donnée particulière tout en continuant à être opérationnelle.

Nous avons présenté les principes et les critères à utiliser pour arriver à caractériser l'environnement du système et, de manière ultime, à générer des courbes de dépendance entre infrastructures essentielles. Le fait de ne pas présenter le mode d'opérationnalisation de ces principes est volontaire. En effet, le mode d'opérationnalisation et d'obtention des informations nécessaires à la création des courbes de dépendance doit être laissé libre aux gestionnaires de réseau. De ce fait, l'important est de créer un espace de coopération et d'échange de manière à faire ressortir les liens particuliers pouvant exister entre différentes infrastructures essentielles. Il s'agit également de décider quel type de courbe de dépendance serait le plus utile. Il existe en effet plusieurs manières de traiter et de présenter le même type d'information.

Une fois l'environnement du système caractérisé, il faut se recentrer sur le système. La caractérisation de l'environnement permet de définir les conséquences de la défaillance d'un système et même d'identifier des composantes particulières de ce système. En effet, en utilisant les zones de fourniture, il est également relativement facile de déterminer les composantes du système situées à l'interface avec l'environnement.

C'est à partir de ces composantes particulières qu'il est possible de débuter la caractérisation du système.

5.2.2 Caractérisation du système

La caractérisation du système permet d'analyser la vulnérabilité interne c'est-à-dire de déterminer les composantes minimales nécessaires pour remplir la ou les missions du système. La caractérisation du système doit commencer à son point de contact, son interface avec son environnement. Il faut, en effet, considérer le système comme une entité utilisant et fournissant des ressources provenant ou allant dans l'environnement. De ce fait, le système doit être analysé et caractérisé entre ces points d'échange avec l'environnement.

Cette analyse s'effectue de manière déductive. Il s'agit de partir des courbes de dépendance définies précédemment de manière à caractériser correctement le système. La caractérisation de l'environnement est effectuée en se basant sur la mission du système et en considérant des zones de fourniture et des caractéristiques d'utilisation d'une ressource. Cette caractérisation de l'environnement permet donc de déterminer un premier point de contact du système avec son environnement. En effet, il est possible d'identifier une infrastructure particulière et une fonction du système qui sont associées à chacun des secteurs de fourniture. C'est à partir de ces fonctions particulières que peut débuter la caractérisation du système.

À l'instar de la caractérisation de l'environnement, la caractérisation du système se base sur différents critères. Le système peut être défini comme le regroupement de fonctions permettant de réaliser sa ou ses missions. Pour effectuer ses fonctions, le système est formé d'un réseau de composantes (infrastructures et équipements) reliées par des liens physiques. En ce sens, le système peut être vu comme une entité bicouche avec la couche fonctionnelle regroupant les fonctions à réaliser et la couche physique caractérisée par les infrastructures et les équipements permettant de supporter le flux des ressources à l'intérieur du système.

En se concentrant sur les liens physiques entre infrastructures essentielles, quatre étapes peuvent permettre de caractériser un système :

- une analyse fonctionnelle ;
- un organigramme technique ;
- la caractérisation de l'état des composantes du système ;
- l'agrégation de ces états.

5.2.2.1 Réalisation d'une analyse fonctionnelle

Une analyse fonctionnelle permet de caractériser la couche des fonctions du système. Comme nous l'avons vu dans le chapitre 4, une fonction peut être définie comme une subdivision organisationnelle d'un système correspondant à un regroupement d'activités ou de tâches qui sont orientées vers un objectif commun. En fait, les différentes fonctions d'un système contribuent à l'exploitation d'un système de manière à remplir sa mission.

Pour débuter la caractérisation du système étudié, il faut donc définir le mode d'organisation des fonctions qui le constituent. Pour cela, il faut effectuer une analyse fonctionnelle interne qui permettra, entre autres, de visualiser sous forme d'un arbre de fonctionnement le mode de succession des différentes fonctions du système comme nous l'avons montré au chapitre 4 dans l'exemple portant sur un aménagement hydroélectrique (Figure 4.4). Différentes fonctions peuvent être définies suivant le mode d'organisation ou de gestion du système.

Il est évident que ce mode d'organisation peut varier suivant le système considéré. En particulier si le système en question comporte des missions particulières et donc des fonctions particulières.

Pour guider la réalisation de l'analyse fonctionnelle interne permettant d'identifier les fonctions techniques, il est possible de suivre les étapes suivantes :

- définir les objectifs et la portée de l'analyse ;
- identifier les fonctions du système ;
- identifier les interactions entre les fonctions du système.

La définition des objectifs et de la portée de l'analyse permet de poser les bases de l'analyse, présentées ci-dessous. Pour cela, il suffit de se poser quelques questions :

- est-ce que l'ensemble des fonctions du système sera étudié ?
- est-ce que seules les fonctions principales seront étudiées ?
- est-ce que seules les fonctions de soutien seront étudiées ?
- est-ce que seules les fonctions présentes dans un secteur donné seront étudiées ?

Cette étape permet également de préciser pour quelle mission du système l'analyse fonctionnelle est effectuée. De manière plus spécifique suivant le type de liens considérés (physique, géographique, cybernétique ou logique), certaines fonctions seront plus importantes à considérer que d'autres.

Une fois le cadre de l'analyse déterminé, il faut identifier les fonctions et déterminer le niveau de raffinement à atteindre.

De manière classique, les fonctions minimales d'un système sont liées à l'utilisation de ressources primaires, à leur transformation avant leur fourniture à d'autres systèmes. Ces fonctions minimales sont les fonctions de production/transformation, de transport, de stockage et de distribution. Ces fonctions sont reliées par un flux de matières ou un flux de ressources. D'autres fonctions sont nécessaires au bon fonctionnement de tout système. Ce sont des fonctions de soutien. Ces fonctions sont de manières classiques les fonctions de maintenance/entretien, de protection, d'administration et de contrôle. Les fonctions de soutien à l'instar des fonctions de base sont importantes à considérer dans le

cadre de l'analyse des vulnérabilités d'un système en relation avec des interdépendances physiques entre infrastructures essentielles. Cependant, elles s'avèrent primordiales pour la considération des vulnérabilités liées aux liens cybernétiques (contrôle) et aux liens logiques (administration).

Comme nous l'a montré le chapitre 4, la représentation de l'analyse fonctionnelle peut se faire sous forme arborescente ce qui permet au gestionnaire du système de visualiser l'évolution des ressources à l'intérieur du système. Pour construire cet arbre, il suffit de considérer l'enchaînement des fonctions du système en relation avec le flux de ressources.

La première représentation est simple et linéaire à tout le moins si ne sont considérées que les fonctions de base. Toutefois, l'arbre peut être plus complexe si les fonctions de soutien sont intégrées et surtout si chacune des fonctions est décomposée en ses activités et tâches constitutives.

L'analyse fonctionnelle devrait se limiter dans un premier temps à la considération des fonctions. La prise en compte des activités et des tâches qu'elles regroupent ne devrait se faire que dans le cas d'analyse régionale. En effet, si l'analyse considère le système dans sa globalité, il est bon de se limiter aux grands types de fonctions. La considération des opérations relatives à chaque fonction devrait s'effectuer pour faire ressortir un besoin particulier en ressources et plus spécifiquement des infrastructures ou des équipements ayant potentiellement un impact sur le système et sur son environnement.

Une fois que les fonctions à considérer ont été déterminées, l'étape suivante consiste à caractériser les liens existants entre elles. De manière classique, les fonctions de base (production, transformation, stockage, transport, distribution) sont reliées par des liens physiques. La ressource ou les ressources passent d'une fonction à une autre sans qu'il y ait véritablement possibilité d'un retour en arrière. Les fonctions de stockage, de transport et de distribution sont particulières, car

elles peuvent impliquer des liens géographiques tant avec l'environnement qu'à l'interne du système.

Les fonctions de soutien sont intégrées au système par des liens physiques, mais également par des liens cybernétiques et logiques. D'ailleurs, pour analyser des interdépendances particulières et par le fait même des vulnérabilités spécifiques, telles que celles reliées à l'utilisation d'outils cybernétiques, il peut être intéressant de se focaliser sur une fonction donnée plutôt que d'effectuer une analyse fonctionnelle globale sur l'ensemble du système. Pour les vulnérabilités cybernétiques, la fonction principale à considérer est la fonction de contrôle qui nécessite des données provenant de toutes les fonctions du système, mais également de l'environnement. Pour ce qui est des liens logiques, la fonction à privilégier au niveau de l'analyse fonctionnelle est l'administration du réseau.

Une fois l'analyse fonctionnelle réalisée, il faut considérer les interactions entre les fonctions du système et le réseau d'infrastructures qui permet de remplir ces fonctions. Pour cela, il faut réaliser un organigramme technique.

5.2.2.2 Réalisation d'un organigramme technique

Comme nous l'avons vu dans le chapitre 4, un organigramme technique permet de définir les infrastructures et les équipements qui constituent un système. Cet organigramme peut et doit être rattaché à l'analyse fonctionnelle qui a été réalisée sur le système. Un exemple d'organigramme technique, réalisé pour l'usine de production d'eau potable de la ville de Montréal, est présenté au chapitre 4 (Figure 4.3). L'intérêt de réaliser un organigramme technique est de compléter les informations récoltées en réalisant l'analyse fonctionnelle. L'objectif étant toujours de caractériser l'organisation du système, mais surtout d'identifier les interactions avec l'environnement (entrée et sortie de ressources). L'organigramme technique permet d'analyser la deuxième couche du système à savoir la couche structurelle.

En partant de la dernière infrastructure du système servant à la fourniture de la ressource produite par le système, il s'agit de construire un arbre de fonctionnement considérant l'ensemble des infrastructures du système. La constitution de cet arbre peut se baser sur les principes qui sont à la base de la construction des arbres de causes qui correspondent à une méthode déductive d'analyse de risques.

Les arbres de causes ont deux objectifs principaux :

- déterminer les diverses combinaisons possibles d'événements entraînant la réalisation d'un événement unique indésirable aussi appelé événement de tête ou événement sommet ;
- représenter graphiquement ces combinaisons au moyen d'une structure arborescente.

Au lieu de considérer comme départ de l'arbre, un événement face auquel nous voulons nous prémunir, il suffit de considérer comme tête de l'arbre, l'infrastructure se trouvant à l'interface entre le système et son environnement pour ce qui est de la fourniture de la ressource.

Les arbres de causes sont constitués en considérant des niveaux successifs d'événements, chaque événement étant généré à partir des événements de niveau inférieur. Les différents niveaux d'événements sont reliés entre eux par des portes logiques.

Pour la caractérisation du système, nous proposons d'utiliser les notions de niveaux successifs et de portes logiques. Bien évidemment, au lieu de considérer des successions d'événements, nous déterminerons des successions d'infrastructures et d'équipements.

Trois types d'infrastructures peuvent être définis :

- l'infrastructure de tête ;
- l'infrastructure intermédiaire ;
- l'infrastructure de base.

L'infrastructure de tête est l'infrastructure à partir de laquelle va être construit l'arbre. Cette infrastructure se situe à l'interface entre le système et son environnement. C'est au niveau de cette infrastructure que la ressource fournie par le système va entrer dans l'environnement. En fait, l'infrastructure de tête correspond à l'endroit où la ressource sort du système.

Les infrastructures intermédiaires sont les infrastructures dont le fonctionnement est nécessaire pour alimenter l'infrastructure de tête. En fait, les infrastructures intermédiaires sont les différentes infrastructures supportant les fonctions du système de manière à alimenter l'infrastructure de tête.

Les infrastructures de base, à l'instar de l'infrastructure de tête, sont des infrastructures qui se situent à l'interface entre le système et son environnement. Elles correspondent à des points d'entrée dans le système des ressources que ce dernier utilise, mais surtout, ces infrastructures sont les dernières infrastructures de la chaîne logistique à appartenir au système.

En fait, pour construire et structurer l'arbre de fonctionnement, il faut considérer une sorte de flux de ressources qui entrent dans le système, transitent dans le système où elles sont transformées avant d'en ressortir. L'arbre de fonctionnement correspond donc à une sorte de diagramme de flux regroupant les infrastructures et équipements d'un système.

Une fois les infrastructures composant le système identifiées, il faut déterminer les relations qui existent entre elles. Pour cela, il est possible d'utiliser le principe des portes logiques.

Les portes logiques à utiliser pour la représentation graphique sont déterminées en s'interrogeant sur la manière dont les infrastructures sont reliées entre elles. En partant de l'infrastructure de tête, il faut se demander quelles autres infrastructures sont nécessaires pour son fonctionnement. Une fois ces infrastructures déterminées, il faut se demander si elles ont toutes la même importance. Si c'est le cas, les infrastructures peuvent être reliées par une porte ET. Par contre, si une infrastructure peut se substituer à une autre, une porte OU peut être utilisée. Une porte CONDITION peut être utilisée si les infrastructures peuvent se substituer partiellement les unes aux autres.

Les portes logiques utilisées nous renseignent donc sur le mode de fonctionnement et de robustesse du système. En effet, plus le nombre de portes ET vont être présentes dans l'arbre et moins le fonctionnement du système sera robuste (c'est l'inverse de l'analyse classique avec un arbre des causes). En effet, la présence des portes OU ou des portes de CONDITION indique les infrastructures redondantes et permet de visualiser les éléments de protection et de substitution mis en œuvre pour renforcer le réseau. Par contre, si les portes ET prédominent, cela veut dire que la dégradation de l'état ou la défaillance d'une infrastructure donnée se répercutera plus rapidement aux infrastructures qui dépendent d'elle.

Ce mode de représentation permet également de faire ressortir des infrastructures ayant des importances particulières. C'est le cas notamment si une infrastructure donnée est unique et est indispensable pour différentes infrastructures qui lui sont reliées.

Il est possible d'utiliser d'autres types de portes logiques et de définir d'autres types d'infrastructures de manière à faire ressortir d'autres types d'information. Un exemple d'information qui peut être intéressant est l'indication des conditions qui pourraient faire qu'une infrastructure se substitue à une autre.

À chaque niveau d'infrastructures ou à chaque infrastructure, il faut associer une matrice donnant des informations complémentaires qui permettent de favoriser la gestion des mesures d'urgence ou de continuité opérationnelle.

La construction de l'arbre de fonctionnement couplée à l'élaboration de matrices permet de mieux comprendre le système et d'identifier ses zones de faiblesse. En effet, le fait qu'une des composantes du système soit indispensable dans le sens où elle est nécessaire pour la réalisation d'une mission donnée du système et qu'elle est la seule pouvant remplir sa fonction (le système ne dispose pas de composante pouvant se substituer à elle) constitue une vulnérabilité du système. La dysfonction ou la défaillance d'une telle composante influera directement sur la dégradation de l'état du système.

Cependant, il faut garder à l'esprit que l'arbre de fonctionnement obtenu dépend du niveau d'analyse et du raffinement choisis. En effet, bien souvent, chacune des composantes d'un arbre de fonctionnement peut elle-même donner lieu à un autre arbre de fonctionnement. Il revient donc au gestionnaire du système de définir à quel niveau d'analyse s'arrêter dépendamment de l'objectif qu'il s'est fixé pour l'analyse des vulnérabilités et pour le renforcement de son système. Il est évident que plus fine sera l'analyse et plus le niveau de connaissance du système sera important. Cependant, cela induira forcément un coût temporel et monétaire plus grand pour faire l'analyse. De plus, il est possible de se demander si une étude très fine du système sera véritablement bénéfique pour contribuer à son renforcement. Dans notre contexte d'étude, le raffinement de l'arbre de fonctionnement devrait s'arrêter lorsqu'aucun nouveau besoin de ressource ne peut être identifié.

D'autre part, il est possible qu'une composante donnée du système soit nécessaire pour différentes missions ou fonctions du système et qu'en cela elle fasse partie de différents arbres de fonctionnement. Cette information pourrait être compilée dans la matrice rattachée à la composante. Cette donnée est primordiale, car elle indique

l'importance de la composante pour le fonctionnement du système et donc la sensibilité du système à la défaillance de cette composante.

La création d'un arbre de fonctionnement est intéressante, car elle peut également permettre de définir le chemin minimal qui correspond aux sous-ensembles d'éléments ou de composants dont le bon fonctionnement simultané assure le bon fonctionnement du système. Cette notion de chemin minimal permet de visualiser la robustesse du système étudié en termes de fonctionnement sans se focaliser sur les événements qui pourraient engendrer la défaillance du système. En effet, il s'agit de déterminer comment la variation d'état d'une composante peut influer sur l'état du système.

Il est évident que pour caractériser un système plusieurs arbres de fonctionnement pourraient être nécessaires. Il faut compter au minimum un arbre de fonctionnement par mission du système voir par zone de fourniture déterminée lors de l'étape de caractérisation de l'environnement du système.

Comme nous venons de le voir, le système peut être subdivisé en composantes techniques pour comprendre son fonctionnement et identifier une partie de ses éléments sensibles. Cette compréhension du système, et par le fait même de ses faiblesses, vient en complément de l'analyse du niveau fonctionnel du système à savoir le niveau des fonctions et des opérations. Ce niveau est directement lié au niveau technique puisque les composantes du système sont mises en œuvre pour remplir les fonctions du système et de manière ultime ses missions.

Une fois l'analyse fonctionnelle et l'organigramme technique du système réalisés, le système est mieux compris. En particulier, ces deux éléments permettent d'identifier les composantes importantes du système (infrastructures et fonctions). Ces éléments importants correspondent aux points sensibles du système et donc à sa vulnérabilité interne dans le sens où la défaillance de ces composantes induira obligatoirement la dysfonction du système et ultimement sa défaillance.

Lorsque les éléments rendant le système vulnérable sont identifiés, il faut caractériser leur état et comment la variation de cet état peut se répercuter sur l'état du système ou plus précisément sur l'état des missions du système.

5.2.2.3 Caractérisation de l'état des composantes

Pour chacune des composantes, déterminées comme étant importantes à partir de l'analyse fonctionnelle et de la réalisation de l'organigramme technique, il faut déterminer la succession des états possibles.

À l'instar de la caractérisation de l'état des ressources fournies, il s'agit donc de définir la succession de l'état de chacune des composantes du système en fonction d'un critère qualitatif ou quantitatif donné.

Quelle que soit la composante considérée, comme nous l'avons spécifié au chapitre 3, trois états de fonctionnement peuvent être définis :

- état normal ;
- état dégradé ;
- état hors-service.

Il faut donc arriver à développer des courbes d'évolution d'état du même type que celles développées pour la caractérisation de l'environnement du système. Ceci semble évident pour les infrastructures constituant le système puisque les premiers critères de caractérisation pouvant être utilisés sont les critères de conception (durée de vie et caractéristiques techniques). En fait, il est relativement aisé de déterminer une droite de variation d'état tel que nous l'avons montré au chapitre 3. Il est cependant plus difficile d'anticiper les facteurs de variation qui pourraient influer sur la pente de la droite de variation et donc sur les délais entre les changements d'état. Il faut également pouvoir caractériser cette variation d'état en fonction du temps, tel que nous l'avons montré dans le chapitre 3.

Ceci n'est pas véritablement problématique dans le sens où la constitution de ces courbes ne constitue qu'un outil d'aide à la décision. Elles ne doivent pas se substituer, mais bien venir compléter des systèmes de veille. La veille permettra en effet de voir un changement dans la pente de la droite de variation d'état de la composante considérée. Elle devrait donc permettre d'anticiper un changement de la marge de manœuvre disponible pour le gestionnaire de l'infrastructure essentielle.

Les critères à utiliser pour caractériser et analyser la variation d'état d'une fonction sont plus difficiles à définir. En effet, pour une fonction, aucun critère de conception ne peut être utilisé pour évaluer la variation des états possibles d'une fonction. Il est toutefois possible d'utiliser des critères de rendement, tel que le pourcentage de réalisation des activités ou des tâches prescrites. L'objectif demeure toutefois le même. Il s'agit de définir le mode de variation d'états, mais aussi d'anticiper le délai restant avant un changement éventuel d'état. Il est également possible de penser que l'état d'une fonction donnée du système est directement relié aux états des infrastructures et équipements qu'elle utilise. Il est possible, dans un premier temps, de considérer que l'état d'une fonction donnée est la résultante directe des états des infrastructures et équipements qui sont nécessaires à sa réalisation. Il est évident que la réalité n'est pas si simple. Il faudra donc, dans un deuxième temps, considérer les effets des règles de gestion et de l'implication de l'humain dans l'évolution de l'état d'une fonction.

Cependant, plusieurs courbes d'évolution de l'état d'une fonction peuvent être réalisées. Tout dépend de l'objectif de l'étude et donc des critères d'évaluation qui seront utilisés.

Une fois les courbes de variations d'état des composantes importantes du système élaborées, deux choses doivent être faites :

- déterminer comment combiner les variations d'états des différentes composantes, comment elles varient les unes par rapport aux autres ;
- déterminer comment ces variations d'états vont influer sur l'état de la mission du système.

Pour cela, il faut définir les principes permettant de combiner les états des composantes à un moment donné, mais aussi d'anticiper les variations d'état d'une composante en relation avec celles qui lui sont liées.

5.2.2.4 Agrégation des états des composantes du système

Il s'agit d'analyser et de caractériser la manière dont la variation de l'état des composantes du système peut influer sur la réalisation de sa mission. Pour cela, il faut tout d'abord comprendre comment les états des différentes composantes du système influent entre elles.

Il s'agit donc de définir à un temps T, les états de toutes les composantes du système qui ont été définies comme importantes par la réalisation de l'analyse fonctionnelle et de l'organigramme technique. Par la suite, il faut définir comment la variation de ces états influe sur l'état du système et donc sur l'état de la ressource qu'il fournit.

Cette approche peut sembler relativement simple si nous considérons qu'une fonction nécessite l'utilisation d'une seule infrastructure (Figure 5.7). Par exemple, la fonction stockage peut ne nécessiter qu'un réservoir.

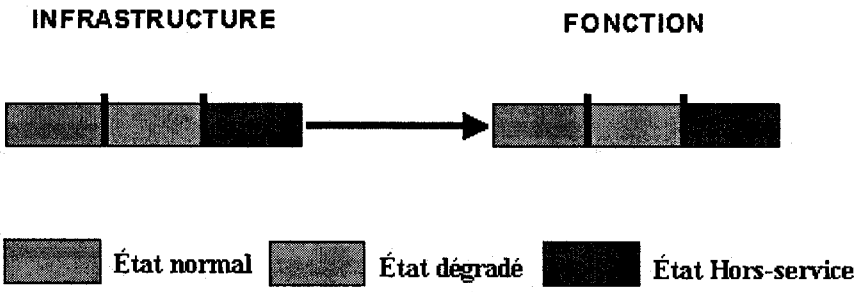

Figure 5.7 - Enchaînement simple des états.

En effet, dans ce cas, l'état de la fonction est directement lié à l'état de l'infrastructure. Donc, si l'infrastructure est dans un état normal, elle n'affectera pas l'état de la fonction. Il est évident que ce n'est pas aussi simple étant donné que d'autres facteurs (aléas) peuvent influer sur l'état de la fonction.

De la même manière, le fait que l'infrastructure soit hors service amènera automatiquement la mise hors service de la fonction à moins qu'il n'y ait des mesures de protection mises en œuvre. Nous pouvons donc présumer, dans une première approche, qu'il en est de même pour la propagation d'un état dégradé de l'infrastructure vers la fonction.

Cependant, l'organisation de tout système est nettement plus complexe. Une fonction utilise dans la majorité des cas plusieurs infrastructures ou équipements. Les infrastructures à considérer sont celles qui auront été déterminées comme étant importantes à la suite de la réalisation de l'organigramme technique. Les fonctions à considérer sont celles qui constitueront le chemin minimal défini suite à la réalisation de l'analyse fonctionnelle.

Cela revient donc à analyser un système complexe où diverses combinaisons d'états de composantes peuvent se traduire par un effet similaire sur l'état du système (Figure 5.8).

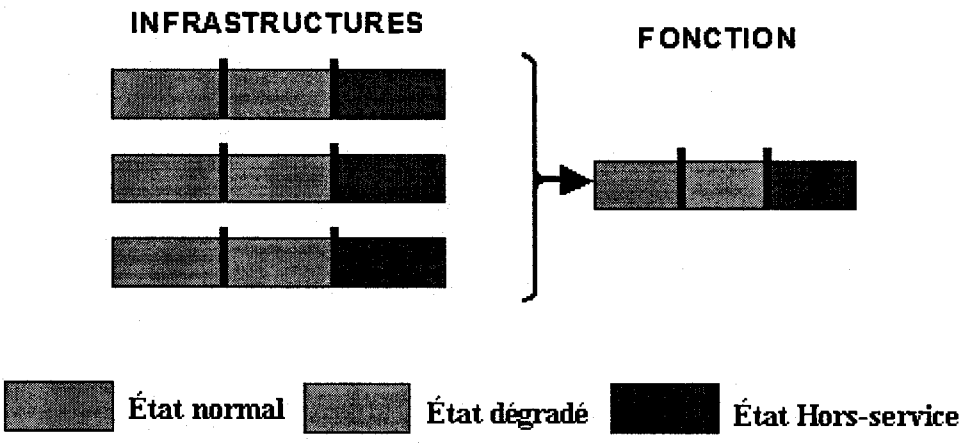

Figure 5.8 - Enchaînement complexe des états.

Le cas de la Figure 5.8 ne se présente que lorsque l'utilisation en parallèle d'infrastructures est nécessaire pour soutenir une fonction donnée. Dans le cas où des infrastructures sont utilisées en série, alors la variation d'état d'une infrastructure agira sur une autre et ainsi de suite jusqu'à ce que la fonction soit affectée. Le système peut alors être analysé en se basant sur la Figure 5.7.

Quand plusieurs infrastructures sont nécessaires pour réaliser une fonction, il faut donc considérer l'état de chacune des infrastructures pour déterminer comment l'état de la fonction va être affecté. Pour cela, il est plus simple que toutes les composantes considérées soient analysées en utilisant le même critère. De plus, pour un gestionnaire d'infrastructure essentielle, le critère temporel semble le plus intéressant, car il permet d'utiliser la notion de marge de manœuvre.

Cinq cas de figure existent pour considérer la répercussion des états des infrastructures sur une fonction donnée :

1. si toutes les infrastructures sont dans un état normal, la fonction sera elle aussi dans un état normal ;
2. si toutes les infrastructures sont dans un état hors service, la fonction sera elle aussi hors service ;

3. si toutes les infrastructures sont dans un état dégradé, la fonction sera elle aussi dans un état dégradé. Il est possible de dire cela puisque nous considérons que toutes les infrastructures ont la même importance, en raison de la manière dont elles ont été définies en utilisant un organigramme technique ;
4. si une infrastructure est dans un état dégradé, la fonction sera elle aussi dans un état dégradé ;
5. si une infrastructure du système est hors service, la fonction sera elle aussi hors-service.

Ces règles d'agrégation permettent déjà au gestionnaire de mettre en œuvre des mesures de surveillance et éventuellement d'éviter une dégradation de l'état de son système.

En fait, la relation, entre les états des infrastructures et l'état de la fonction, est plus complexe dans le sens où d'autres facteurs peuvent affecter l'état de la fonction considérée. Mais, toujours dans un esprit d'initier le processus, nous pouvons nous limiter à l'affectation de l'état de la fonction par l'état des infrastructures qui lui sont nécessaires. Une fois que ces relations seront analysées, le processus pourra être raffiné et intégrer d'autres aléas ou facteurs de variation.

La relation entre les états des infrastructures et l'état de la fonction est cependant plus difficile à caractériser quand les infrastructures ne sont pas toutes dans le même état. En effet, il ne suffit pas de déterminer dans quelle classe d'état se retrouve la fonction analysée, mais bien de déterminer quel délai sépare l'état actuel de la fonction du prochain seuil de changement d'état. Cette problématique se pose uniquement quand les variations d'état sont caractérisées en termes de temps ou lorsque les critères utilisés sont qualitatifs. Il s'agit donc de définir dans quelle classe d'état se trouve la fonction, mais également quelle marge de manœuvre sépare l'état actuel du prochain état.

En fait, la difficulté principale consiste à bien caractériser le passage d'un état à un autre. Cette difficulté tient à la manière dont vont être définies les limites et les transitions entre les classes d'état (Figure 5.9).

Les transitions entre les classes peuvent être de trois grands types (stricte, courbe ou selon une droite).

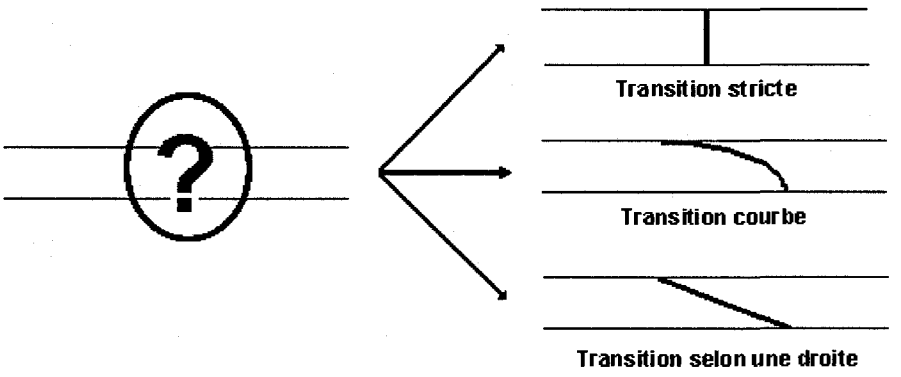

Figure 5.9 - Différents modes de transition entre deux classes d'état.

Si la limite est stricte, il n'y aucune incertitude sur l'état dans lequel se trouve une composante donnée. Le changement d'état s'effectue en effet à une valeur précise. Dans ce cas-là, les règles simples d'agrégation que nous avons définies peuvent être utilisées. L'état d'une fonction donnée sera le même que l'état le plus contraignant des infrastructures qui lui sont nécessaires.

Dans les deux autres cas de transition (courbe ou selon une droite), à l'approche de la transition, la composante considérée va se retrouver dans deux états différents. Par exemple, elle pourra ne pas être totalement en état normal ou en état dégradé, mais dans un état à la fois normal et dégradé.

Dans un contexte d'aide à la décision, il est possible de considérer que la composante est dans un autre état dès lors que son état approche de la zone de

transition. Il est par exemple possible de considérer qu'une composante donnée est en état dégradé dès qu'elle est dans un état incertain à la fois normal et dégradé. Raisonner de cette manière présente l'avantage de forcer la proactivité de l'analyse du système et la mise en œuvre de mesures d'atténuation appropriées. L'inconvénient principal est qu'il est alors possible de raisonner en fonction de phénomènes non avérés ce qui se traduit par la mise en œuvre de procédures non nécessaires.

Ce mode de raisonnement semble toutefois intéressant en termes de mesures d'urgence. Il permet en effet d'anticiper les problèmes éventuels et d'ainsi se préparer à réagir adéquatement. En effet, le fait de se trouver dans une zone de transition peut montrer une certaine fragilité du système. Il montre surtout que le système tend vers une augmentation de sa défaillance et donc vers un changement d'état.

Cette indication du changement éventuel d'état pourrait être raffinée en levant l'incertitude entourant les zones de transition. Le mode d'agrégation d'états de différentes composantes pourrait également être amélioré en définissant des règles plus précises.

Pour cela, une des solutions possibles consiste à utiliser les principes de la logique floue. Il n'est pas nécessaire de développer des modèles mathématiques complexes visant à retranscrire la réalité, mais bien d'anticiper une évolution pouvant paraitre imparfaite, mais suffisante pour aider le gestionnaire d'un système à prendre des décisions dans un cadre de continuité opérationnelle ou de mesures d'urgence.

La logique floue permet de caractériser un certain degré d'incertitude. La logique floue développée par Zadeh (1965) sert à pouvoir expliquer un phénomène en se basant sur la théorie des ensembles flous. L'objectif ultime étant de pouvoir développer des programmes informatiques permettant à des ordinateurs de contrôler des processus comme pourrait le faire un humain. Il s'agit donc, dans un

certain sens, d'essayer de représenter l'organisation des connaissances et donc de caractériser un phénomène comme le ferait un expert.

Le principe de la logique floue part d'une constatation relativement simple à la base. Un élément donné peut appartenir à plusieurs sous-ensembles flous. Cet élément peut donc être caractérisé par une fonction et un degré d'appartenance à ces sous-ensembles sans pour cela utiliser des probabilités (Dehail, 2003). Les exemples les plus souvent utilisés pour illustrer ce phénomène sont la vitesse d'une automobile et la température de l'eau. Dans ces deux cas, il existe des règlements ou des lois physiques qui permettent de poser des limites strictes. Si nous prenons le cas de la vitesse d'une voiture, il existe des limitations de vitesse sur autoroute au Québec, la vitesse minimale est de 60 km/h et la vitesse maximale est de 100 km/h. Cependant, la vitesse de 100 km/h peut-elle être qualifiée d'élevée ? Un être humain va utiliser différents paramètres (état des routes, moment de la journée, trafic, ses capacités, son type de voiture, etc.) pour déterminer à quelle vitesse rouler et si cette vitesse de 100 km/h est élevée ou non. La logique floue essaye de formaliser ce mode de raisonnement de l'être humain de manière à caractériser le pourcentage d'appartenance d'une vitesse à différentes classes, telles que vitesse élevée, vitesse moyenne et vitesse faible.

Dans une approche de logique floue, il est donc important de définir le type de classes ou de sous-ensembles flou qui permettent de caractériser un phénomène, mais aussi de définir les limites entre ces classes et leurs types (stricte, linéaire ou courbe) (Dehail, 2003). Une fois cela fait, il faut caractériser des degrés d'appartenance à ces classes. C'est ce qui est appelé la quantification floue.

Cette approche semble donc bien adaptée à notre problématique. En effet, toutes les composantes d'un système sont caractérisées en fonction de la variation de leur état. Nous avons défini trois états possibles à savoir normal, dégradé et hors service. Il faut essayer de définir des limites ou des seuils fixes (limites strictes) pour caractériser le passage d'un état à un autre. De cette manière, l'état de la

composante appartiendra toujours à 100% à une classe donnée. Cependant, comme nous l'avons montré, les limites ne sont pas si fixes que cela, les changements d'état peuvent survenir un peu avant ou un peu après un seuil.

Dans un premier temps, quand une composante appartient à deux classes différentes, il peut s'avérer suffisant de considérer que cette composante appartient à 100 % à la classe d'état la plus défaillante. Cela permet de se préparer adéquatement en mettant en place les procédures nécessaires au rétablissement du système. Toutefois, plus les transitions entre les classes seront bien définies, plus la fonction d'appartenance à différents états sera précise et plus l'analyse pourra l'être également. Les modes d'intervention seront donc plus précis et les modes d'action plus adaptés à la situation anticipée.

La logique floue devrait également permettre de raffiner les modes d'agrégation. Dans une première approche, nous avons défini que si l'ensemble des composantes nécessaires à une mission étaient dans un état donné (ex. : dégradé), alors la mission serait dans le même état (dégradé). Nous avons également posé comme principe que l'état le plus contraignant d'une composante déterminerait l'état de la mission reliée. Ces principes de base ne sont pas forcément vrais. L'utilisation des principes de la logique floue basée sur l'expertise de spécialistes du fonctionnement des systèmes permettra de lever l'incertitude entourant la combinaison des états des composantes et de leur répercussion sur l'état de la mission qu'ils supportent.

La combinaison de l'utilisation de l'analyse fonctionnelle, de la réalisation d'un organigramme technique, des critères d'agrégation devrait permettre de caractériser la relation entre états des infrastructures, états des fonctions et état de la mission du système (Figure 5.10). La logique floue pourrait également permettre de raffiner les modes d'agrégation des états des différentes composantes du système analysé.

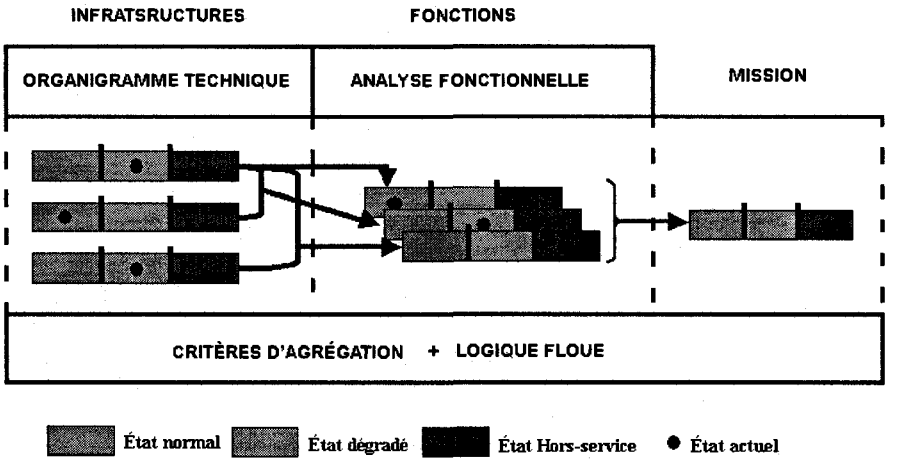

Figure 5.10 - Caractérisation du système.

Actuellement, les travaux réalisés par le *Centre risque & performance* caractérisent le système en déterminant des ensembles fonctionnels. Guichardet (2009) définit ces ensembles fonctionnels comme la combinaison d'une ou plusieurs ressources utilisées, des infrastructures importantes pour la réalisation d'une ou plusieurs fonctions et de la ressource qu'elle sert à fournir sur un secteur donné. Le but de définir des ensembles fonctionnels est de déterminer l'état d'une ressource fournie en fonction de l'état d'une ressource utilisée par une infrastructure essentielle sans pour autant faire une étude de l'état de l'ensemble des composantes du système. Pour cela Guichardet (2009) définit des modes d'affectation de même que les composantes les plus importantes d'un système pour la réalisation de sa mission.

Cette approche ne nécessite donc pas, pour le moment, d'analyser les variations d'états des composantes du système de même que le mode d'agrégation de ces états. En définissant les ensembles fonctionnels, cette méthode propose de relier directement l'état d'une ressource fournie sur un secteur de fourniture à l'état d'une ou plusieurs ressources utilisées sur des secteurs d'utilisation. La détermination de l'effet des composantes du système est laissée sous la responsabilité des experts du système. Il s'agit donc plus de colliger les informations importantes comme le

feraient des experts de manière à anticiper la variation d'état des ressources fournies et par le fait même des effets domino pouvant potentiellement être engendrés.

Nous pensons que les concepts que nous proposons, pour analyser les variations d'état des composantes d'un système et donc sa vulnérabilité interne, demeurent intéressants et valides. Cependant, ils restent pour le moment assez difficiles à mettre en œuvre spécifiquement en raison du niveau d'information qu'ils demandent. Cette gestion de l'information pourrait être facilitée par le développement d'un système expert utilisant les principes de l'endorsement. Nous présenterons plus en détail ces principes pour la détermination de la vulnérabilité amont du système.

Les états des composantes du système vont varier en relation avec différents facteurs, tels que leurs âges et les pressions de l'environnement. Toutefois, parmi tous ces facteurs de changement, il en existe un type qui est prépondérant dans le sens où il est indispensable tant pour le fonctionnement normal que pour le fonctionnement en situation d'urgence du système. Il s'agit des besoins du système et donc de l'utilisation des diverses ressources nécessaires pour son fonctionnement.

Il faut donc caractériser les besoins du système et déterminer comment leur variation d'états peut influer sur les états des composantes du système.

5.2.3 Caractérisation des besoins du système

En se focalisant sur le fonctionnement d'un système, nous pouvons poser comme hypothèse de travail que la variation de l'état du système dépend exclusivement de la satisfaction de ses besoins. La satisfaction des besoins correspond alors à l'utilisation de ressources. Les ressources peuvent être de natures diverses. Comme nous l'avons précisé au chapitre 4, six types de ressources peuvent être définis (Robert et coll. 2007). Parmi ceux-ci, un nous intéresse plus particulièrement à

savoir la ressource information et données. Cette ressource peut également être qualifiée de ressource cybernétique.

C'est donc au niveau de la caractérisation des besoins du système qu'intervient véritablement la prise en compte de l'élément cybernétique. Mais, il faut tout d'abord définir ce que nous entendons par cybernétique.

L'utilisation du terme cybernétique peut être trompeuse en français. En effet, il est utilisé pour caractériser deux concepts reliés, mais relativement différents.

5.2.3.1 La cybernétique : science du gouvernement

La première signification, et celle qui est la plus largement admise, réfère à la discipline qui examine les rapports de similitude et de différence entre les processus biologiques (dirigés par le cerveau humain) et les processus techniques (dirigés par les appareils mécaniques, électriques ou électroniques), en vue de les ramener à des principes de base communs (Office québécois de la langue française, 2008). La cybernétique est donc vue comme la science du gouvernement (du grec *Kubernetike*, art de gouverner) qui est orientée vers le contrôle, la régulation et la communication (Lalonde, 2005).

La cybernétique correspond alors à un processus de transfert d'information qui peut se caractériser par quatre éléments principaux (Lalonde, 2005) :

- une action, un transfert d'information par un émetteur vers un récepteur ;
- une rétroaction, la répercussion de l'information sur l'ensemble du système ;
- une régulation qui correspond au potentiel de stabilisation du système ;
- une capacité d'adaptation du système face à l'imprévu.

L'action correspond au transfert d'une information significative entre des composantes d'un système. Elle correspond en quelque sorte à une relation de causalité où une composante A va être en relation avec une composante B.

La rétroaction correspond à la considération de l'affectation de la composante A par la composante B. Cette rétroaction correspond à la fois à un retour d'information de la composante B vers la composante A, mais également à un transfert de cette information vers les autres composantes du système.

En fait, l'action et la rétroaction sont à la base du modèle de communication émetteur-récepteur (Figure 5.11).

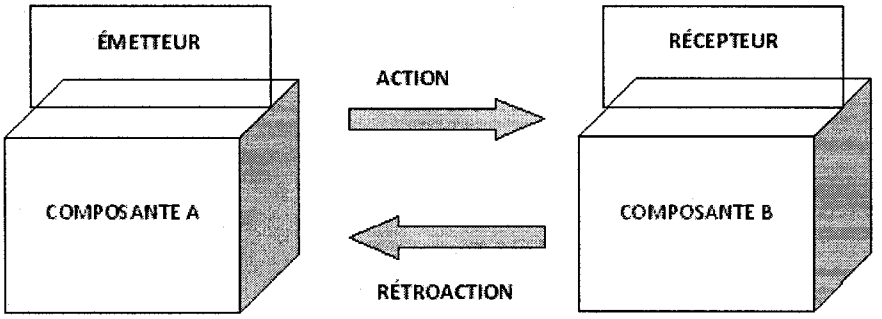

Figure 5.11 - Modèle de communication émetteur - récepteur.

Ce modèle est bien sûr prépondérant en termes de communication et d'échange, mais il est aussi extrêmement intéressant pour la caractérisation d'un système. En effet, il permet de caractériser à la fois les interactions existantes entre les composantes d'un système, mais également celles existantes entre le système et son environnement.

La notion de rétroaction permet entre autres de considérer la recherche d'un état de stabilité du système (rétroaction négative) et la possibilité de changement d'état du système (rétroaction positive). Cette recherche d'un état de stabilité du système peut être considérée comme une composante de la résilience du système à savoir sa capacité à retrouver un état de fonctionnement acceptable après une dégradation.

La régulation vient compléter la notion de rétroaction en spécifiant que la conservation ou la transformation du système sont issues du même processus. En

fait, l'évolution du système est contrainte par les pressions de son environnement et par l'évolution de chacune de ses composantes. L'évolution du système est donc directement reliée aux informations dont il dispose et de celles qui lui sont transmises. La cybernétique correspond donc à un processus de considération de l'évolution et du changement du système.

LeMoigne (1990) précise que le système et son évolution peuvent être évalués suivant quatre dimensions :

- les fonctions ;
- les environnements ;
- les transformations ;
- les finalités du système.

Le système est alors vu comme un ensemble d'actions dans un environnement qui sert à réaliser des projets. Ce système fonctionne et peut se transformer.

Nous voyons donc que, d'après la définition de LeMoigne (1990), la cybernétique correspond déjà à une évaluation du système tel que nous l'avons défini. L'évolution du système peut en effet être caractérisée par son environnement, sa mission, ses composantes (infrastructures et fonctions) et les évolutions de leurs états.

L'adaptation traduit la capacité du système à retrouver un état d'équilibre avec son environnement. Ce concept traduit bien la manière dont se comporte un environnement naturel. Cette recherche d'équilibre peut sembler plus difficile à concevoir pour un système technique ou un système humain. Cependant, il est certain que les systèmes développés par l'homme sont fortement connectés, les interdépendances entre infrastructures essentielles en sont un parfait exemple. De plus, il est facile de vérifier que la variation de l'état d'une infrastructure essentielle va directement affecter les autres infrastructures essentielles qui lui sont reliées.

Les différentes infrastructures essentielles et donc les différents systèmes vont évoluer simultanément de manière à retrouver un état d'équilibre.

La cybernétique, dans son sens premier, mène donc à la caractérisation des échanges d'information entre des systèmes. De ce fait, elle constitue une part importante de l'approche systémique.

5.2.3.2 La cybernétique : sécurité informatique

La deuxième signification de la cybernétique est directement reliée à la sécurité informatique. En effet, dans ce cas, le terme cybernétique est souvent utilisé pour qualifier la sécurité ou les éléments concernant l'informatique de manière générale et Internet de manière spécifique. Au Canada, le centre chargé de la surveillance des menaces et de la coordination des interventions suite aux incidents concernant la cybersécurité s'appelle d'ailleurs le Centre canadien de réponse aux incidents cybernétiques (SPC, 2008f). Les termes sécurité cybernétique et incident cybernétique sont donc utilisés comme traduction des termes anglais « *cyber incident* » ou « *cyber security* ». Cette utilisation du terme cybernétique est trompeuse. Il est donc préférable de lui préférer le préfixe « cyber » qui réfère au cyberespace.

Dans ce travail, l'utilisation du terme cybernétique réfère à son sens premier. La cybernétique est donc vue comme un moyen d'analyser un système en se basant sur les transferts d'information.

5.2.3.3 Prise en compte de la cybernétique

Un élément cybernétique peut donc être défini comme un élément relié au transfert et à l'utilisation d'information et de données. Cet élément est particulièrement important dans la société actuelle et pour les sociétés futures. En effet, les systèmes techniques, et en premier lieu les infrastructures essentielles, sont de plus en plus complexes. Toutes les actions à mener pour opérer ces systèmes ne peuvent pas se faire manuellement. Ces systèmes sont donc de plus en plus automatisés et opérés à

distance. Cette manière de procéder nécessite donc des flux importants de données qu'il faut stocker, mais surtout traiter. Ces quantités d'informations sont tellement importantes qu'il peut devenir difficile de savoir exactement l'information dont le système dispose, mais surtout de voir si une information est altérée ou pas. Il faut donc caractériser la donnée comme un besoin, une ressource nécessaire au bon fonctionnement d'un système.

Les besoins du système en données se font sentir au niveau de ses fonctions. Les données sont principalement de trois types (Redman, 1998) :

- les données opérationnelles utilisées pour le fonctionnement quotidien d'un système ;
- les données tactiques utilisées par des fonctions de gestion routinière, mais pas nécessairement journalière ;
- les données stratégiques utilisées pour les décisions à long terme.

La différenciation des types de données (opérationnelle, tactique et stratégique) donne déjà une indication sur le délai d'affectation des fonctions qui utilisent des données.

Ces trois types de données sont particulièrement importants pour le bon fonctionnement d'un système. Toutefois, dans un contexte de mesures d'urgence et de continuité opérationnelle, il faut tout d'abord se concentrer sur les données opérationnelles et tactiques qui peuvent affecter rapidement le système en se répercutant sur son état. En fait, il s'agit de se concentrer sur la dépendance du système à l'utilisation courante de données.

La prise en compte de l'influence des données stratégiques sur l'état du système est également importante. Cependant, il n'est pas utile de les considérer dans un contexte de gestion courante du système. Par contre, il est évident que l'effet sur l'état du système des décisions stratégiques et des données utilisées devra être

considéré dans le sens où il affectera sans aucun doute le fonctionnement du système par une modification des processus.

Il faut donc définir, pour chacune des fonctions du système, quelles sont les informations nécessaires à son opération. Une fois les types de données nécessaires définis, il faut les trier en termes d'importance pour la fonction considérée.

Il est possible de définir deux classes de données :

- les données critiques dont la défaillance aura un impact direct et immédiat sur l'état d'une fonction ;
- les données de soutien dont la défaillance aura un impact sur l'état d'une fonction sans pour autant être immédiat.

Les critères pour différencier ces deux classes sont donc :

- le temps, le délai durant lequel la fonction peut se passer d'une information ou d'une donnée sans que son état ne soit affecté ;
- l'importance de l'impact de la dégradation de la donnée sur le fonctionnement du système.

L'importance des données donne donc une indication sur le délai disponible avant que la ou les fonctions utilisant les données n'entrent en dysfonction.

Une fois les données classées suivant leur importance pour le système ou plus exactement en termes de dépendance du système face à l'obtention des données, il faut qualifier l'état des données et donc leur qualité.

La qualité peut être définie comme « l'ensemble des caractéristiques d'une entité qui lui confèrent l'aptitude à satisfaire des besoins exprimés ou implicites » (UIT-T, 2005, page 3).

Du point de vue des données, cette qualité peut être différenciée en deux types :

- la qualité de fonctionnement ;
- la qualité de service.

La qualité de fonctionnement est « l'aptitude d'un réseau ou d'un élément du réseau à assurer les fonctions liées à des communications entre usagers » (UIT-T, 2005, page 5). La qualité de fonctionnement réfère donc aux modes de transfert des données.

Le mode de fonctionnement des systèmes engendre des vulnérabilités de sécurité. Ces vulnérabilités peuvent se concrétiser par une perte voir une dégradation des données. Selon le type de vulnérabilité, les conséquences peuvent se faire ressentir à plus ou moins longue échéance.

La Figure 5.12 présente les types de vulnérabilités auxquels peut faire face un système en termes de qualité de fonctionnement de même que des actions pouvant utiliser ces vulnérabilités.

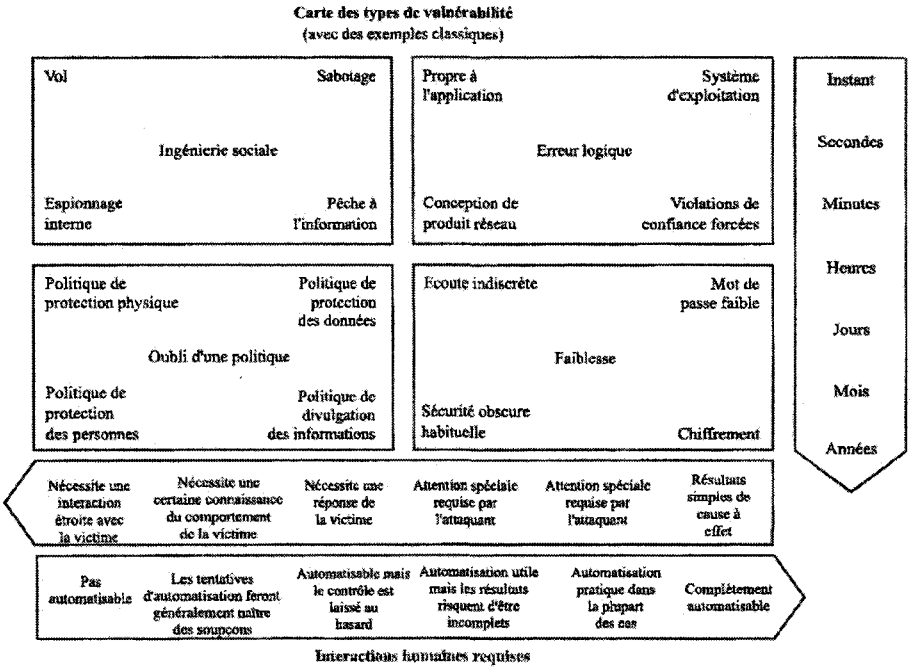

Figure 5.12 - Décomposition de la nature des vulnérabilités. (UIT-T, 2005).

La vulnérabilité est donc vue ici comme un défaut présent dans la sécurité d'un système informatique. L'Union internationale des télécommunications définit quatre types de vulnérabilités pouvant être exploités pour affecter un système (UIT-T, 2005) :

- ingénierie sociale ;
- oubli d'une politique ;
- erreur logique ;
- faiblesse (défaut de conception du système).

L'ingénierie sociale réfère principalement aux actes de malveillance (vol, sabotage et espionnage) qui pourraient affecter le fonctionnement du système. L'oubli d'une politique réfère directement à la mauvaise application d'un politique interne qui a pour but de protéger l'intégrité et la divulgation des informations sensibles. L'erreur logique et la faiblesse caractérisent plus les problèmes de conception et d'opération des systèmes informatiques ce qui pourrait conduire à leur dégradation.

Ces quatre types de vulnérabilité vont avoir des effets plus ou moins immédiats dans le temps. Par exemple, un vol pourra affecter le système immédiatement tandis que l'effet d'un problème de chiffrement ne sera détectable qu'à long terme. De plus, comme le montre la Figure 5.12, en considérant l'interaction avec l'humain, nous constatons que ces vulnérabilités nécessitent, pour être exploitées, une connaissance plus ou moins poussée des systèmes.

Ces vulnérabilités sont donc fonction de leur cible (humain ou système informatique) et de la durée nécessaire pour que la vulnérabilité soit exploitée (Tableau 5.1).

Tableau 5.1 - Les quatre vulnérabilités fondamentales (UIT-T, 2005).

	Concerne une personne	**Concerne un système informatique**
Instantané	Ingénierie sociale	Erreur logique
Nécessite un certain temps	Oubli d'une politique	Faiblesse

Ces quatre types de vulnérabilité, de même que leur délai d'affectation du système, sont des éléments qui doivent être pris en compte dans une méthodologie d'analyse des vulnérabilités cybernétiques. Ces éléments sont en fait les critères qui vont permettre de caractériser la qualité de fonctionnement du système.

La sécurité informatique cherche à protéger les systèmes informatiques face aux intrusions et aux actes de malveillance en général. Cet élément est très important dans un contexte de continuité opérationnelle, mais il n'est pas le seul devant être considéré.

Il faut également considérer l'aspect de sûreté de fonctionnement. Pour cela, Il faut donc analyser comment la qualité de service peut affecter les fonctions d'un système donné.

La qualité de service est « l'effet global produit par la qualité de fonctionnement d'un service qui détermine le degré de satisfaction de l'usager du service » (UIT-T, 2005, page 3). La qualité de service est donc représentative des accords pris entre un fournisseur et un utilisateur en ce qui a trait à la fourniture d'une ressource. En ce sens, la qualité de service permet de caractériser le mode d'affectation du fonctionnement d'un système par rapport aux modes de dégradation possible d'une donnée.

Certaines caractéristiques permettent de définir la notion de qualité de service :

- le débit de transfert (vitesse de transfert) des données ;
- le temps d'attente ;
- la précision des données ;
- la qualité de fonctionnement.

La qualité de fonctionnement influe directement sur la qualité de service puisque la dégradation du mode de transfert des données va obligatoirement se traduire par une dégradation des données et par le fait même du degré de satisfaction des usagers.

La qualité de fonctionnement (transfert de flux de données) peut agir sur quatre critères permettant de caractériser les données :

- la disponibilité ;
- la confidentialité ;
- l'intégrité ;
- l'authenticité.

La Figure 5.13 montre comment le flux de données peut être affecté et entraîner la dégradation de la qualité des données.

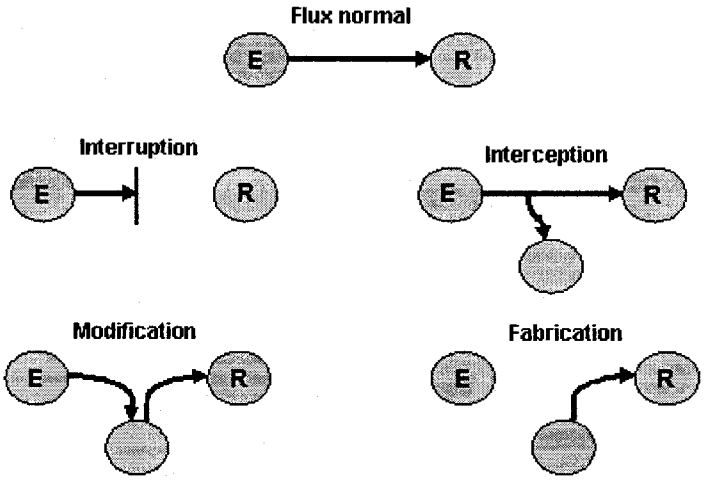

Figure 5.13 - Menaces de sécurité (UIT-T, 2005).

De manière normale et dans une approche cybernétique, un émetteur (E) émet un flux de données qui se rend jusqu'à un récepteur (R).

L'interruption du flux d'information fait que les données ne se rendent pas au récepteur. L'interruption du flux affecte donc la disponibilité de la ressource cybernétique.

L'interception du flux d'information fait que les données sont captées entre l'émetteur et le récepteur. L'interception du flux affecte donc la confidentialité de la ressource cybernétique.

La modification du flux d'information fait que les données sont transformées (dégradées) avant d'arriver au récepteur. La modification du flux affecte donc l'intégrité de la ressource cybernétique.

La fabrication du flux d'information fait que les données qui arrivent au récepteur ne proviennent pas du bon émetteur. La fabrication du flux affecte donc l'authenticité de la ressource cybernétique.

Ces critères permettant de caractériser la qualité de service doivent également être pris en compte dans une méthodologie d'évaluation des vulnérabilités cybernétiques d'un système.

Normalement, pour vérifier la qualité des données, l'approche la plus courante est la détection et la correction des erreurs. Cela revient à s'assurer que les bases de données utilisées sont correctes. Une autre approche consiste à s'assurer qu'aucune donnée incorrecte ou redondante ne soit intégrée à la base de données.

Cependant, dans le but de caractériser l'affectation d'une fonction par la dégradation de la qualité des données utilisées, il semble utile de déterminer comment l'évolution de qualité d'une donnée peut affecter l'état d'une fonction du système.

Pour cela, il est possible d'utiliser les principes de l'endorsement. Il s'agit alors d'analyser les conditions qui pourraient mener à la dégradation de l'état du système comme le ferait un expert.

La théorie de l'endorsement est une théorie de gestion de l'incertitude définie par Cohen (1986). Cette théorie vise à déterminer des classes de condition permettant de caractériser un événement donné. Il est possible de définir plusieurs classes de condition.

Cependant, comme le souligne Robert (1989), il peut être suffisant de définir uniquement trois classes :

- les conditions exclusives qui entraînent le rejet de l'événement ;
- les conditions nécessaires qui sont les conditions menant à la réalisation de l'événement ;
- les conditions supportives qui renforcent la certitude d'existence de l'événement.

Si nous appliquons la théorie de l'endorsement à la problématique de la cybernétique, il faut tout d'abord définir quel événement nous allons analyser. Comme nous voulons caractériser la manière dont des données affectent les fonctions d'un système, le plus simple est de définir notre événement comme la dysfonction d'une fonction donnée. Il est ainsi plus facile de définir les trois classes de conditions (exclusives, nécessaires et supportives).

Les conditions exclusives sont les conditions qui feraient que la fonction analysée serait en état normal ou optimal. Dans ce cas, la dégradation d'une donnée n'affecterait pas l'état d'une fonction. Pour la prise en compte de la dépendance d'une fonction face à l'utilisation d'une donnée, les conditions exclusives sont les conditions qui correspondent à un état normal voir optimal des données et de leur utilisation par le système. En fait, les conditions exclusives correspondent au fait que les critères caractérisant les données et leur utilisation par le système sont optimales pour un bon fonctionnement du système. Par exemple, une condition exclusive serait qu'une donnée *opérationnelle importante* pour une fonction du système soit en *état normal* et que son *flux de transfert* soit *normal.*

Les conditions nécessaires sont les conditions qui conduisent automatiquement à la dysfonction de la fonction analysée. Ce sont donc les conditions indispensables pour que la dégradation d'une donnée se répercute sur l'état d'une fonction. Par exemple, une condition nécessaire pourrait être le fait qu'une donnée *opérationnelle importante* pour une fonction du système soit dans un état *dégradé.*

Cette condition entraînera nécessairement un changement d'état de la fonction qui utilise la donnée. De manière concrète, une condition nécessaire pourrait être la détection erronée de la hauteur d'eau dans un barrage ce qui pourrait engendrer une mauvaise gestion des évacuateurs de crue.

Les conditions supportives sont les conditions qui renforcent la certitude en ce qui a trait à la dysfonction de la fonction analysée. Une condition supportive pourrait donc faire que la dégradation d'une donnée se répercute sur l'état d'une fonction. Par exemple, une condition supportive pourrait être le fait qu'une donnée *opérationnelle utile* pour une fonction du système soit dans un état *dégradé*. Cette condition n'entraînera pas forcément un changement d'état de la fonction qui utilise la donnée. Cependant, combinée avec d'autres conditions supportives, elle pourrait contribuer à la dégradation de l'état de la fonction qui l'utilise. Si nous gardons l'exemple de l'opération d'un ouvrage hydroélectrique, une condition supportive pourrait être l'obtention tardive d'une alerte météo. Le fait que le temps se dégrade n'engendrera pas directement la défaillance du barrage mais pourra l'accélérer si la mesure du niveau d'eau est défaillante.

La détermination des conditions d'endorsement est très importante. Les conditions exclusives sont primordiales car elles permettent d'accélérer la réflexion et la prise de décision. Pour l'application aux besoins du système, les conditions exclusives permettent de savoir que tous les signaux sont au vert et donc que le système fonctionne de manière optimale dans son environnement. Les conditions nécessaires et supportives permettent d'anticiper la dégradation de l'état du système et ultimement sa mise hors-service.

La théorie de l'endorsement est donc développée pour essayer de caractériser si un événement va se concrétiser en s'interrogeant à savoir si les conditions pouvant conduire à sa réalisation sont présentes.

Il s'agit donc de déterminer les conditions qui peuvent mener à la variation d'état d'une fonction en relation avec la qualité des données utilisées. À ce moment-là, il est possible d'utiliser les trois classes de condition telles que définies par Robert (1989). Les classes correspondront alors aux critères de caractérisation de la qualité des données.

Ces critères doivent se baser sur les notions de qualité de service et de qualité de fonctionnement. Les critères constituant les conditions doivent également reprendre les critères qui ont permis de différencier les données critiques des données de soutien (Tableau 5.2).

Tableau 5.2 - Critères de caractérisation des données.

	Critères
Relation données/fonction	• Types de données : → Opérationnelles ; → Tactiques ; → Stratégiques. • Importance des données : → Délai avant l'affectation de la fonction ; → Degré d'affectation de la fonction.
Qualité de fonctionnement : Qualité du Flux/transfert des données	• Type de vulnérabilités : → Ingénierie sociale ; → Oubli d'une politique ; → Erreur logique ; → Faiblesse du système. • Menaces de sécurité : → Flux normal ; → Interruption ; → Interception ; → Modification ; → Fabrication.
Qualité de service : Qualité des données	• Disponibilité ; • Confidentialité ; • Intégrité (État) ; • Authenticité ; • Débit de transfert ; • Temps d'attente.

L'état de la donnée (normal, dégradé ou hors-service) n'est donc qu'un des critères à considérer pour caractériser l'affectation d'une fonction relativement à son utilisation de données. Cet état ne constitue donc qu'une des conditions pouvant engendrer une variation de l'état de la fonction.

Le Tableau 5.2 montre également que pour la caractérisation de la qualité des données et leur mode de répercussion sur l'état d'une fonction, la notion de temps est prépondérante. Elle intervient en effet à différents niveaux. La notion de délai intervient tant sur la qualité de service que sur la qualité de fonctionnement et sur l'importance des données pour la fonction.

Il est évident que les conditions (exclusives, nécessaires et supportives) vont également varier suivant le niveau d'état anticipé de la fonction. L'événement à considérer est de manière générale la dysfonction de la fonction. De manière spécifique, cet événement peut être subdivisé suivant les deux états possibles de cette dysfonction (dégradé ou hors service).

Il est possible de déterminer diverses conditions :

- Les conditions qui vont mener à un état normal de la fonction.
  Ces conditions sont la prise en compte de tous les critères qui vont faire que le fonctionnement du système va être optimal et que ses besoins vont être remplis adéquatement. Ce sont les conditions exclusives.
- Les conditions qui vont mener à un état dégradé de la fonction.
  Ces conditions correspondent à des variations dans les critères de la caractérisation des données et de leur nécessité pour le système qui vont entraîner la dégradation de l'état fonctionnel du système. Ce sont donc des conditions nécessaires ou supportives pour que le système soit en état dégradé.
- Les conditions qui vont mener à un état hors service de la fonction.
  Ces conditions correspondent à des variations dans les critères de la caractérisation des données et de leur nécessité pour le système qui vont entraîner la mise hors service du système. Ce sont donc des conditions nécessaires ou supportives pour que le système soit en état hors service.

En déterminant les conditions nécessaires et supportives, il est possible de caractériser l'évolution de l'état d'une fonction suivant son utilisation des données. L'utilisation de l'endorsement permet d'analyser la relation entre états des données et état de la fonction. En effet, l'état d'une donnée est un des éléments pouvant engendrer un changement d'état d'une ou de plusieurs fonctions.

Pour déterminer ces conditions d'endorsement, nous devons utiliser l'information à notre disposition à savoir :

- le mode d'utilisation d'une donnée par une fonction. Pour déterminer cette relation, nous utilisons le type et l'importance de la donnée pour la fonction (Tableau 5.2) ;
- l'état de la donnée. Pour déterminer cet état, nous utilisons les critères définissant la qualité de fonctionnement et la qualité de service (Tableau 5.2).

Considérons que nous analysons une fonction F_1 qui utilise deux types de données D_1 et D_2 qui sont toutes les deux des données opérationnelles c'est-à-dire qu'elles sont utilisées de manière quotidienne pour le fonctionnement du système. Dans notre cas, cela veut dire que la fonction F_1 a besoin de ces données D_1 et D_2 sur une base journalière.

La donnée D_1 est critique pour le fonctionnement de la fonction F_1, c'est-à-dire que cette donnée a un impact direct et immédiat sur l'état de la fonction F_1.

La donnée D_2, quant à elle, est une donnée de soutien pour la fonction F_1, c'est-à-dire que l'impact de cette donnée sur l'état d'une fonction F_1 ne sera pas immédiat.

En connaissant ces particularités des données D_1 et D_2 et en utilisant leur état possible (normal, dégradé ou hors service), il est possible de définir des conditions d'endorsement. Le Tableau 5.3 montre des exemples de ces conditions d'endorsement.

Tableau 5.3 - Exemple de conditions d'endorsement.

Conditions	Donnée				Fonction	
	Nom	État	Type	Importance	Nom	État
Exclusive	D_1	N	Opérationnel	Critique	F_1	N
Nécessaire	D_1	D	Opérationnel	Critique	F_1	D
Supportive	D_2	HS	Opérationnel	Soutien	F_1	N
Nécessaire	D_1	D	Opérationnel	Critique		
Supportive	D_2	HS	Opérationnel	Soutien	F_1	HS

Si la donnée D_1 est dans un état normal (N), alors la fonction F_1 sera en état normal (N). Le fait que la donnée D_1 soit en état normal constitue donc une condition exclusive lorsque nous analysons la dysfonction possible de la fonction F_1.

Si la donnée D_1 est dans un état dégradé (D), alors la fonction F_1 sera en état dégradé (D). Le fait que la donnée D_1 soit en état dégradé constitue donc une condition nécessaire pour la dysfonction de la fonction F_1.

Si la donnée D_2 est dans un état hors service (HS), cela n'aura aucune répercussion sur la fonction F_1. Par contre, si la donnée D_1 est dans un état dégradé (D) et que la donnée D_2 est dans un état hors service (HS), alors la fonction F_1 sera en état hors service (HS). Le fait que la donnée D_2 soit en état dégradé (D) constitue donc une condition supportive pour la dysfonction de la fonction F_1. Elle renforce la certitude en ce qui a trait à la dysfonction de la Fonction F_1. Cette condition prise seule n'aura aucun effet sur la Fonction F_1. Par contre, si elle est combinée à une condition nécessaire ou à une condition supportive, elle peut conduire à l'augmentation de l'état de dégradation de la Fonction F_1.

Il est évident que les conditions d'endorsement choisies peuvent être complexifiées par l'intégration de plus de critères de caractérisation des conditions.

Il est également évident que la même combinaison de critères peut constituer une condition nécessaire pour une fonction donnée et être une condition supportive pour une autre fonction. La Figure 5.14 illustre cette problématique :

- l'état de la donnée D_1 est une condition nécessaire à la variation d'état de la fonction F_1 ;
- l'état de la donnée D_2 est une condition nécessaire à la variation d'état de la fonction F_2 et est une condition supportive à la variation d'état de la fonction F_1 ;
- l'état de la donnée D_3 est une condition supportive à la variation d'état de la fonction F_3 ;
- l'état de la donnée D_4 est une condition nécessaire à la variation d'état de la fonction F_4 et une condition supportive à la variation d'état de la fonction F_3.

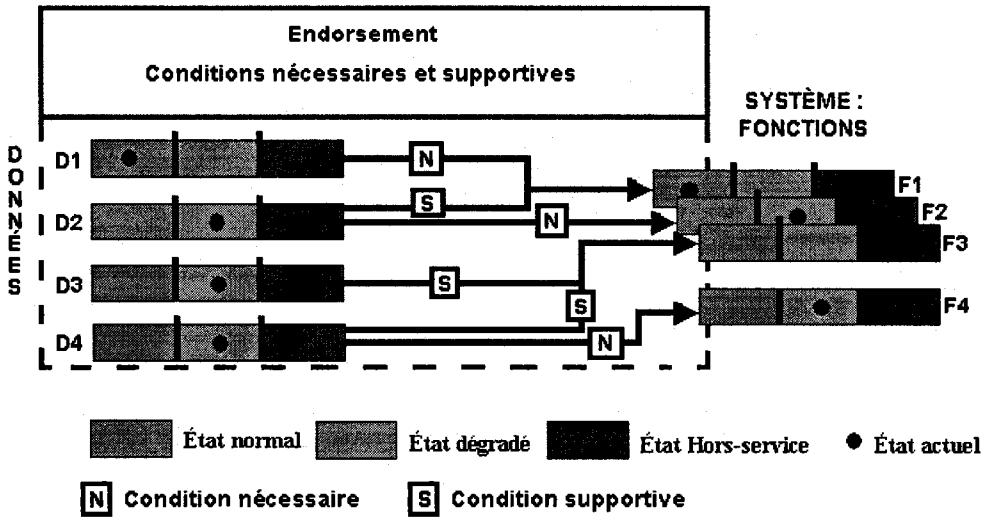

Figure 5.14 - Caractérisation des besoins cybernétiques.

La variation des états de ces données ne vont donc pas avoir les mêmes répercussions sur l'ensemble des fonctions du système.

L'état dégradé de la donnée D_2 n'aura aucune incidence sur la fonction F_1 puisque la donnée D_1, qui constitue la condition nécessaire à la dégradation de l'état de la fonction F_1, est dans un état normal.

Par contre, l'état dégradé de la donnée D_2 va entraîner la dégradation de l'état de la fonction F_2. La dégradation de l'état de la donnée D_2 est donc une condition nécessaire à la dégradation de l'état de la fonction F_2 alors qu'elle constitue une condition supportive pour la dégradation de l'état de la fonction F_1.

Les états dégradés des données D_3 et D_4 vont se répercuter sur l'état de la fonction F_3. Les états dégradés des données D_3 et D_4 sont des conditions supportives qui combinées entraînent la mise hors-service de la fonction F_3. Si une de ces données étaient en état normal, la fonction F_3 n'aurait pas été affectée.

L'état de la donnée D_4 se répercute directement sur l'état de la fonction F_4 puisque cet état est une condition nécessaire pour la dégradation de l'état de la fonction F_4.

En définissant correctement les conditions d'endorsement et leur mode de combinaison, il est donc possible de caractériser l'état d'une fonction (événement) en fonction des états attendus des données qui sont nécessaires à son fonctionnement.

Il est évident que la relation entre l'état des données et l'état des fonctions peut être raffinée en définissant des conditions intégrant plus de critères présentés au Tableau 5.2. Il faut en particulier intégrer les critères de qualité et de délai de transfert des données.

L'endorsement est donc un outil primordial qui permet de combiner des conditions qui vont permettre de caractériser l'effet de combinaison de données sur différentes fonctions du système. L'endorsement permet donc d'agréger les effets des données.

De plus, l'utilisation des principes de l'endorsement permet de définir quand la variation d'état de la fonction s'effectuera en raison de la prise en compte des notions de temps dans l'établissement des conditions.

Cette étape de caractérisation des besoins cybernétiques peut être complétée en générant des courbes de dépendance. Ces courbes permettraient de relier les besoins d'un système en termes cybernétiques avec les capacités de fourniture en données d'un autre système.

Actuellement, l'utilisation de l'endorsement pour la caractérisation de la dépendance d'un système et plus exactement de ses fonctions face à l'utilisation des données cybernétiques n'a pas encore été appliquée à un cas pratique.

À la fin des trois étapes de caractérisation, les relations et les effets des changements d'état des besoins du système en ressources cybernétiques jusqu'à celui des missions du système seront caractérisés.

L'étape suivante consiste à mettre en place un système de surveillance et de suivi qui permettra de s'assurer de la justesse des principes posés, mais aussi de raffiner les conditions et les modes d'agrégation proposés.

5.2.4 Processus d'amélioration continue

La quatrième et dernière phase de la méthodologie consiste en un raffinement des caractérisations effectuées. C'est une phase de surveillance et de suivi qui va permettre de :

- s'assurer de la validité des caractérisations effectuées ;
- intégrer les nouvelles informations disponibles ;
- considérer l'évolution du fonctionnement du système ;
- considérer l'évolution de l'environnement.

La phase d'amélioration du processus permet, en définitive, de s'assurer de la mise à jour des interactions existantes tant à l'intérieur du système qu'entre le système et son environnement. Cette phase peut permettre également de faire évoluer la méthodologie en intégrant des préoccupations particulières des gestionnaires de système de même que d'autres aléas et les besoins du système autres que cybernétiques. Cette intégration ne devrait pas poser de problème étant donné que nous ne posons que des principes sur lesquels doit se baser une méthodologie d'analyse des vulnérabilités. Ces principes de base demeurent les mêmes. Seuls le temps nécessaire et les types de courbes développées changeront en fonction du cadre d'analyse déterminé.

La méthodologie proposée d'analyse des vulnérabilités ne constitue qu'une première phase d'une gestion efficace des vulnérabilités reliées à une infrastructure essentielle. En effet, deux autres phases doivent être mises en œuvre par la suite :

- une phase d'évaluation des vulnérabilités qui permettra de déterminer des niveaux acceptables de vulnérabilité aval, interne et amont ;
- une phase de maîtrise des vulnérabilités qui permettra de véritablement gérer les vulnérabilités en mettant en œuvre des mesures de protection ou des règles d'opération spécifiques.

La combinaison des trois phases permettra réellement d'assurer la continuité opérationnelle du système.

5.3 Conclusion

Ce chapitre a permis de poser les principes d'une méthodologie d'analyse des vulnérabilités basée sur le mode d'organisation d'un système, tel que défini au chapitre 4 et intégrant les caractéristiques du risque, telles que définies au chapitre 3.

Cette méthodologie se subdivise en quatre étapes :

- la caractérisation de l'environnement dans lequel s'intègre le système ;
- la caractérisation du système ;
- la caractérisation des besoins du système ;
- l'amélioration continue.

La caractérisation de l'environnement du système permet d'analyser la vulnérabilité aval en se focalisant sur la répercussion de la dégradation de la mission du système sur son environnement. Cette vulnérabilité aval est analysée en créant des courbes de dépendances ou des courbes de conséquences basées sur la variation d'état des ressources fournies par le système.

Cette première étape de la méthodologie d'analyse des vulnérabilités est déjà appliquée par le *Centre risque & performance* en particulier pour les villes de Québec et de Montréal. Ces applications abordent plus spécifiquement les interdépendances physiques et géographiques entre infrastructures essentielles.

La caractérisation du système permet d'analyser la vulnérabilité interne du système en se focalisant sur son mode d'organisation structurelle et fonctionnelle. Cette vulnérabilité interne peut être analysée en utilisant des méthodes, telles que les organigrammes techniques ou les analyses fonctionnelles. Ces outils sont relativement classiques dans un contexte industriel. Toutefois, il s'agit ici de définir les composantes importantes du système de manière à évaluer leurs états et leurs modes de répercussion sur l'état de la ressource fournie par le système. Pour cela, nous suggérons d'utiliser des règles simples d'agrégation des états combinées aux concepts de la logique floue permettant la prise en compte d'un certain niveau d'incertitude.

Cette deuxième étape de la méthodologie d'analyse des vulnérabilités n'a pas encore été réellement appliquée à un cas concret. En effet, elle touche à un élément particulièrement sensible concernant la sécurité des infrastructures essentielles.

L'approche proposée s'intéresse directement à l'organisation et jusqu'à un certain point à la localisation des composantes du système. L'important dans ce travail était de définir les éléments à identifier et de proposer une manière de le faire. Le soin du mode d'opérationnalisation de la méthode devrait être laissée libre à chaque gestionnaire de systèmes. De cette manière, le gestionnaire n'est en aucun cas obligé de divulguer les informations sensibles concernant l'organisation de son système. Il aura juste à communiquer l'information pertinente aux autres gestionnaires pour les étapes de caractérisations de l'environnement et des besoins des systèmes. Pour permettre cela, les travaux de Guichardet (2009), réalisés au sein du *Centre risque & performance*, proposent l'utilisation du concept d'ensemble fonctionnel et la détermination des informations pertinentes permettant de supporter le développement d'une base de connaissances. Les principes proposés par Guichardet (2009) permettent, en quelques sortes, de caractériser le système en n'ayant pas à gérer trop d'information ou des données pouvant être sensibles.

La caractérisation des besoins du système permet d'analyser le dernier type de vulnérabilité à savoir la vulnérabilité amont se focalisant sur la variation d'état des ressources nécessaires au fonctionnement du système. Pour cela, les données sont caractérisées en termes de qualité de fonctionnement et de qualité de service. Les principes de l'endorsement sont utilisés pour déterminer le mode de répercussion de l'état des données sur l'état du système.

Cette étape pourrait être complétée par la création de courbes de dépendance qui permettraient de relier deux systèmes en termes de fourniture de besoins.

Cette troisième étape de la méthodologie d'analyse des vulnérabilités est déjà appliquée par le *Centre risque & performance* en particulier pour les villes de Québec et de Montréal. Ces applications abordent plus spécifiquement les interdépendances physiques entre infrastructures essentielles et se focalisent sur les

ressources utilisées par les réseaux partenaires du centre, tels que les réseaux d'électricité, de gaz ou d'eau (Robert and Morabito, 2008).

Toutefois, nos travaux vont plus loin en tenant compte spécifiquement de la cybernétique. Pour cela, les données et l'information sont définies comme un type de ressource particulière pouvant être analysée en termes de variation d'états et de délai d'obtention. De plus, nous proposons également d'utiliser le principe de l'endorsement pour caractériser un degré d'importance des données pour le fonctionnement du système et pour établir un mode d'agrégation des états.

La quatrième étape vise à s'assurer de la validité des caractérisations effectuées. Elle constitue donc un processus d'amélioration continue qui va permettre de raffiner la compréhension des interactions entre les éléments, mais aussi d'intégrer toute évolution de ces éléments.

La méthodologie proposée reprend les points forts des méthodes de sûreté de fonctionnement en favorisant une représentation graphique des résultats et en utilisant des outils tels que l'analyse fonctionnelle. De plus, elle permet également d'éviter certains points problématiques des méthodes actuelles en se basant sur une approche déductive pour les étapes de caractérisation.

Il est par contre évident que l'utilisation des résultats obtenus se fera de manière inductive. À partir du changement d'état d'un des éléments considérés, les interactions et les délais définis lors des étapes de caractérisation permettront d'anticiper l'évolution possible des états de l'ensemble des éléments.

La méthodologie proposée et les principes qui la supportent permettent de répondre aux troisième et quatrième hypothèses de recherche de ce travail.

La troisième hypothèse était que l'analyse de la vulnérabilité d'une infrastructure essentielle pouvait se faire de manière déductive en partant des conséquences de défaillances et en remontant vers les ressources essentielles utilisées par le système.

L'approche proposée répond à cette hypothèse puisqu'en partant de la caractérisation de l'environnement d'implantation d'un système, elle s'attache à définir les causes pouvant potentiellement engendrer des défaillances en considérant les vulnérabilités aval, interne puis amont du système. Il est évident que nous avons vérifié cette hypothèse principalement de manière théorique. Toutefois, les travaux passés (Dehail, 2003 ; Robert et Morabito, 2008) et actuels (Guichardet, 2009) réalisés par le *Centre risque & performance* de l'École Polytechnique de Montréal tendent à confirmer l'applicabilité des principes que nous avons posés.

La quatrième hypothèse était que le risque cybernétique pouvait être analysé en considérant les données comme une des ressources essentielles d'une infrastructure essentielle.

L'approche proposée répond également à cette hypothèse en considérant la cybernétique dans sa définition initiale à savoir un mode de communication et d'échange de données dans un système. De cette manière, il est possible de caractériser et donc d'anticiper la répercussion de la variation d'états d'une donnée ou d'une information sur l'état de fonctionnement du système. Cette hypothèse est vérifiée de manière théorique. Il est évident qu'il reste encore à démontrer son applicabilité pratique.

CHAPITRE 6 DISCUSSION GÉNÉRALE

Ce travail de doctorat a comme but principal de proposer les principes méthodologiques qui permettront d'évaluer la vulnérabilité d'une infrastructure essentielle reliée à l'utilisation de données cybernétiques.

Cette recherche comporte deux orientations. La première est une recherche fondamentale. Elle vise à poser les concepts de risque, mais aussi les bases et les principes permettant de développer une méthodologie d'analyse des vulnérabilités des infrastructures essentielles. Cette partie de la recherche constitue la majeure partie de ce travail.

La deuxième orientation de recherche est une recherche plus appliquée. Elle vise à réfléchir sur l'applicabilité des résultats de la recherche fondamentale. Cette orientation ressort peut-être moins dans le sens où aucune application de la méthodologie dans son ensemble n'a pas été réalisée. Cependant, certains éléments de la méthodologie proposée sont déjà appliqués, comme nous l'avons montré dans les chapitres précédents. De plus, la réflexion sur la définition des concepts présentés dans ce travail a été effectuée en gardant à l'esprit les problématiques et les caractéristiques des infrastructures essentielles de même que les préoccupations des gestionnaires de ces réseaux.

Dans ce chapitre de discussion, nous reviendrons sur les hypothèses posées pour effectuer ce travail et sur leur vérification. Nous nous intéresserons également à l'applicabilité et à l'opérationnalisation des concepts posés et de la méthodologie proposée. Finalement, nous aborderons les travaux qu'il faudrait mener suite à cette recherche.

6.1 Vérification des hypothèses de recherche

Pour ce travail, nous avons posé quatre hypothèses de recherche dont la vérification ou l'infirmation doit permettre de juger de l'atteinte du but principal de cette recherche, mais aussi de sa qualité.

Ces quatre hypothèses de recherche sont :

- **Hypothèse 1 :** le concept de vulnérabilité et la notion d'état d'un système sont des composantes intrinsèques du risque ;
- **Hypothèse 2 :** une infrastructure essentielle peut être définie en fonction de ses missions, fonctions et besoins (ressources essentielles) ;
- **Hypothèse 3 :** l'analyse de la vulnérabilité d'une infrastructure essentielle peut se faire de manière déductive en partant des conséquences de défaillances et en remontant vers les ressources essentielles, se poser la question « Pourquoi/Comment » plutôt que « Et-Si/Comment » ;
- **Hypothèse 4 :** le risque cybernétique peut être analysé en considérant les données comme des ressources essentielles d'une infrastructure essentielle.

6.1.1 Vérification de la première hypothèse

Pour vérifier la première hypothèse, nous avons posé comme objectif de définir les concepts de risque et de vulnérabilité. Cet objectif a été atteint dans le troisième chapitre.

Nous avons défini le risque comme étant une fonction de trois éléments principaux que sont les aléas pouvant affecter un système, l'état du système et les conséquences pouvant être engendrées par la dysfonction du système. Cette façon d'aborder le risque est intéressante dans le sens où elle fait ressortir un élément important qui a tendance à souvent être sous-évalué voir ignoré, l'état du système.

La prise en compte de l'état du système en relation avec les aléas et les conséquences permet également d'introduire d'autres éléments constitutifs du risque qui sont très importants :

- la dysfonction du système ;
- les effets domino ;
- la vulnérabilité.

Les notions de dysfonction et d'effets domino sont intéressantes dans le sens où elles permettent de prendre en compte les répercussions de la défaillance du système sur son environnement. La défaillance du système correspond au fait que le système ne remplit plus sa mission et donc qu'il peut induire des effets directs sur son environnement. Ce sont ces effets qui se traduisent par des conséquences. Les effets domino constituent un deuxième niveau de conséquences. Ils correspondent en fait à des enchaînements de défaillance en cascade qui sont caractéristiques des interrelations entre systèmes.

La notion de vulnérabilité est prépondérante. Cette notion est au cœur du risque dans le sens où elle est directement liée à l'état du système. Cependant, la vulnérabilité est aussi fonction des aléas pouvant affecter le système, mais également des conséquences pouvant être engendrées. De ce fait, la vulnérabilité peut être subdivisée en trois niveaux :

- la vulnérabilité amont qui est fonction des aléas externes et de l'état du système ;
- la vulnérabilité interne qui est fonction des aléas internes et de l'état du système ;
- la vulnérabilité aval qui est fonction de l'état du système et des conséquences engendrées.

Les notions d'état du système et de vulnérabilités permettent de définir deux autres éléments qui sont particulièrement importants dans le domaine de la gestion des

risques et plus spécifiquement de ceux des mesures d'urgence et de la continuité opérationnelle. Ces notions sont la résilience et la marge de manœuvre.

De manière classique, la résilience est vue comme le potentiel d'un système de revenir à un état normal après une défaillance. Cependant, cette notion de résilience apparaît plus complexe dans le sens où elle intègre également le potentiel d'un système à remplir sa mission même si son fonctionnement est dégradé. De plus, la résilience doit également intégrer le fait que le système va, après une défaillance, retrouver un niveau d'équilibre qui ne correspondra pas forcément à l'état du système considéré comme normal avant sa défaillance.

La notion de marge de manœuvre correspond au délai dont dispose le gestionnaire du système avant que le système ne change d'état et qu'il entre en dysfonction, qu'il ne soit plus résilient.

D'un point de vue théorique, notre premier objectif est atteint ce qui permet de dire que notre première hypothèse est valide. En effet, nous avons différencié les concepts de risque et de vulnérabilité qui sont souvent utilisés comme synonyme. De plus, nous avons proposé une définition et une représentation du risque qui permettent d'intégrer tous les concepts prépondérants pour une gestion proactive des risques.

Les définitions proposées permettent également d'introduire les concepts de résilience et de marge de manœuvre.

Le quatrième chapitre portant sur l'organisation du système a également permis de conforter notre première hypothèse dans le sens où nous avons abordé l'organisation du système en nous basant sur les définitions que nous avons posées.

6.1.2 Vérification de la deuxième hypothèse

La deuxième hypothèse porte sur l'organisation du système. L'organisation d'un système est particulièrement importante dans un contexte de gestion des risques. En effet, elle permet de caractériser l'état d'un système, état qui, comme nous l'avons vu, est à la base même de la notion de risque.

Pour vérifier cette hypothèse, nous avons posé deux objectifs :

- caractériser les différents groupes de fonctions constitutives d'une infrastructure essentielle ;
- caractériser les besoins essentiels d'une infrastructure essentielle.

Ces objectifs ont été abordés dans les quatrième et cinquième chapitres de ce travail.

Le chapitre 4 a permis de montrer le mode d'organisation d'un système et comment il est possible en utilisant une succession de questions d'analyser cette organisation. Plus précisément, en utilisant les principes des analyses fonctionnelles et en réalisant un organigramme technique, il est possible de caractériser le système en termes de ressources fournies, missions, fonctions, infrastructures et ressources utilisées. Le chapitre 4 présente des exemples d'analyse fonctionnelle et d'organigramme technique pouvant être réalisés.

Le chapitre 5 a permis de montrer l'intégration de ce mode d'organisation d'un système dans son environnement dans la méthodologie proposée. En effet, chacun des éléments (ressources fournies/missions, fonctions/infrastructures, ressources utilisées) correspond à une étape spécifique de la méthodologie proposée. Ces étapes de caractérisation intègrent, entre autres, les principes à la base des organigrammes techniques et des analyses fonctionnelles.

6.1.3 Vérification de la troisième hypothèse

La troisième hypothèse concerne directement la méthodologie d'analyse des vulnérabilités en proposant qu'une approche déductive puisse être utilisée. Pour vérifier cette hypothèse, l'objectif était de poser les principes de cette démarche.

Le chapitre 5 a abordé spécifiquement le développement d'une méthodologie d'analyse des vulnérabilités d'une infrastructure essentielle. Cette analyse s'effectue en partant des conséquences pouvant être engendrées par la dysfonction d'un système et en remontant vers la dépendance du système aux ressources qu'il utilise.

L'approche proposée est systémique et systématique atteignant donc l'objectif fixé en début de recherche. La méthodologie est systématique dans le sens où elle propose quatre étapes bien définies. Trois de ces étapes sont des étapes de caractérisation centrées respectivement sur les ressources fournies par un système, sur le système lui-même et sur les ressources que le système utilise. Chacune des étapes de caractérisation vise à définir l'état des éléments sur lesquels elle se focalise permettant de cette manière d'évaluer un des trois niveaux de la vulnérabilité (aval, interne et amont). La quatrième étape est une étape de surveillance et de suivi permettant à la fois d'adapter la méthodologie à un contexte précis mais aussi de raffiner les analyses effectuées.

L'approche proposée est également systémique dans le sens où elle aborde les trois niveaux de vulnérabilité et vise à analyser le système (infrastructure essentielle) et ses interactions avec son environnement. La vulnérabilité d'une infrastructure essentielle donnée est donc analysée et évaluée en considérant l'infrastructure essentielle dans son contexte d'implantation. De plus, la méthodologie vise à évaluer les variations d'états des composantes du système en relation avec les variations d'états des ressources utilisées par le système, mais également avec les variations de l'état de la ressource fournie. Cette approche doit permettre d'évaluer l'évolution de chacune des composantes du système et donc du système en général

avec son environnement. Cette manière de procéder devrait permettre grâce à l'étape de l'amélioration continue d'aborder la problématique de la résilience du système. En effet, il sera possible de déterminer la capacité du système à fonctionner en état dégradé, mais également sa capacité de retrouver un état d'équilibre après une défaillance.

6.1.4 Vérification de la quatrième hypothèse

La quatrième hypothèse porte sur la prise en compte de la dépendance du système face à l'outil cybernétique. Elle part du principe que la vulnérabilité cybernétique d'un système peut être abordée comme la dépendance du système à une ressource qu'il utilise à savoir l'information. Pour vérifier cette hypothèse, l'objectif est de définir comment intégrer la cybernétique dans la méthodologie d'analyse des vulnérabilités proposée.

Cet objectif est abordé dans le chapitre 5. Tout d'abord, la définition de la cybernétique a été reprécisée. Le terme cybernétique a été pris dans son sens premier à savoir un processus d'échange d'informations et de capacité d'adaptation d'un système. Il s'agit donc d'aborder le problème du risque cybernétique sous l'angle de la sûreté de fonctionnement et donc des besoins du système en termes d'échange d'information. Pour cela, la méthodologie propose d'utiliser les principes de l'endorsement.

L'objectif semble donc atteint, au niveau théorique, puisque le chapitre 5 a permis de montrer qu'il est possible de considérer les données ou les informations comme des ressources particulières qui sont utilisées par un système. Il est même possible de dire que ce type de ressource est indispensable au fonctionnement d'un système et cela tant en situation normale qu'en situation d'urgence. Les données et les informations sont en effet indispensables en raison des modes de contrôle des systèmes qui sont de plus en plus automatisés, mais également du fait de l'importance des informations pour mettre en œuvre une gestion proactive des risques.

De manière théorique, les quatre hypothèses de ce travail ont été vérifiées. Les objectifs fixés pour permettre de valider ou d'infirmer nos hypothèses ont été atteints. Cependant, il est possible de se demander si les concepts et les principes proposés sont applicables de manière pratique.

6.2 Application de la terminologie et de l'organisation du système proposées

Les troisième et quatrième chapitres de ce travail ont permis de définir une terminologie du risque et de proposer un mode d'organisation des systèmes. De manière théorique, ces définitions et ces concepts semblent bons, mais est-ce que les personnes œuvrant dans le domaine de la gestion des risques et plus spécifiquement les gestionnaires d'infrastructures essentielles sont en accord avec les concepts proposés ?

Pour répondre à cette question, nous allons regarder plus spécifiquement l'applicabilité :

- des définitions que nous avons proposées ;
- de l'organisation du système que nous avons proposé ;
- des étapes de la méthodologie que nous avons proposée.

6.2.1 Les notions de risque, vulnérabilité et résilience

Comme l'a montré le chapitre 3 de ce travail, la définition classique du risque est généralement articulée autour des notions d'aléas et de conséquences. Nous avons intégré une autre notion apparaissant prépondérante, l'état du système analysé. Il est possible de se demander si les professionnels de la gestion des risques peuvent accepter une définition des risques basée sur le triplet Aléas-État du système-Conséquences.

La commission d'enquête sur l'effondrement du viaduc de la Concorde apporte une partie de la réponse à cette question.

En effet, elle rappelle qu'en Amérique du Nord, l'évaluation des ponts utilise deux indices (Johnson et coll., 2007) :

- l'indice d'état qui fait référence aux conditions de la structure. Il mesure le degré de solidité de l'ouvrage ou, dans une perspective inverse, son degré de détérioration.
- l'indice de fonctionnalité qui correspond à la capacité de la structure à fournir à l'usager la ressource qu'il attend d'elle.

Si nous considérons un pont comme un système, l'indice de fonctionnalité réfère donc à la capacité du système à remplir sa mission. L'indice d'état correspond quant à lui, comme son nom l'indique, à une caractérisation de l'état du système.

Si nous réfléchissons en termes de risque d'effondrement du viaduc, nous voyons ressortir les trois notions de base qui nous permettent de définir le risque :

- les aléas qui peuvent déclencher l'effondrement du pont ;
- l'état du pont qui fait qu'il va être plus sensible à certains aléas ;
- les conséquences qui correspondent à l'effondrement de la structure.

La notion d'état est donc très importante à considérer pour analyser et évaluer un risque donné. Elle est indispensable à la bonne gestion des infrastructures civiles. Cette constatation que tire la commission d'enquête sur l'effondrement du viaduc de la Concorde sur l'importance de l'état du pont dans son effondrement semble valide quel que soit le système considéré. En effet, l'état du système et plus spécifiquement la variation d'état du système influe directement sur sa vulnérabilité et sa résilience, tels que nous les avons définis. Ce fait semble évident pour les structures physiques, mais il est valide quel que soit le domaine des risques considérés. Pour cela, il suffit de penser au domaine médical où le système est l'être humain. Les analyses de risque sont basées sur le triplet que nous avons défini. Une étude peut évaluer le développement d'un cancer donné (conséquences), pour des hommes d'un âge donné (état du système) qui fument (aléas).

Cette notion d'état est d'autant plus importante à intégrer dans la considération du risque qu'elle constitue la seule composante du risque portant véritablement sur le système en lui-même.

La deuxième partie de la réponse à la question que nous nous posons quant à l'utilisation possible de notre définition du risque vient de la tendance actuelle à vouloir effectuer des analyses de vulnérabilité de manière à améliorer la résilience des systèmes. La vulnérabilité d'un système est indissociable de la notion d'état du système. De plus, comme l'a montré Blancher (1998), la vulnérabilité est directement liée à trois éléments que nous considérons dans notre définition du risque à savoir les aléas (vulnérabilité amont), le système et son organisation (vulnérabilité interne) et les conséquences sur l'environnement (vulnérabilité aval). D'autre part, le risque tel que nous le définissons permet de véritablement le différencier du concept de vulnérabilité. La vulnérabilité est un des éléments permettant de caractériser le risque.

Les conclusions de la commission d'enquête sur l'effondrement du viaduc de la Concorde de même que le mode de gestion des ponts permettent également de voir la pertinence d'un autre élément que nous prenons en compte dans notre définition du risque. En effet, l'indice de fonctionnalité réfère comme nous l'avons vu à la capacité du système à réaliser sa fonction. Cette caractéristique est directement prise en compte dans notre définition par la notion de dysfonction. Cet élément caractérise le fait que la dégradation de l'état du système peut engendrer des conséquences.

Le dernier élément que nous intégrons dans notre définition du risque est la notion d'effets domino. Comme le montre la revue bibliographique de ce travail, de nombreux travaux se développent actuellement dans le domaine des interdépendances entre infrastructures essentielles. Cette préoccupation démontre l'importance de la prise en compte de ce concept dans une définition du risque.

Les six notions (aléa, vulnérabilité, état, dysfonction, conséquence, effet domino) que nous utilisons pour définir le risque sont de plus en plus utilisées dans les domaines de l'analyse et de la gestion des risques. Ces termes sont donc acceptés, mais il faut se demander si les définitions que nous proposons pour ces termes le sont ou peuvent l'être.

Les travaux effectués par le *Centre risque & performance,* à partir des concepts que nous avons proposés dans ce travail, tendent à laisser penser que oui. Les concepts constitutifs du risque tels que nous les avons définis ont été utilisés dans des projets d'évaluation des interdépendances entre infrastructures essentielles développées pour les villes de Montréal et de Québec (Robert et Morabito, 2009). Ces projets ont donné des résultats pratiques qui sont intégrés dans les activités des infrastructures essentielles. De manière plus spécifique, ces travaux ont permis de développer des outils de gestion proactive des risques qui sont utilisés par les partenaires tant publics que privés du centre. Nous avons donné des exemples, aux chapitres 3 et 5, de courbes de dépendance qui ont été développées lors des travaux du *Centre risque & performance*. En ce sens, les définitions que nous proposons pour les composantes du risque semblent acceptées au niveau opérationnel.

Sachant cela, nous pouvons nous demander si les concepts et les définitions proposées peuvent être acceptés à un niveau stratégique c'est-à-dire à un niveau de décision plus global. Les travaux réalisés récemment par l'Organisation de sécurité civile du Québec (OSCQ) permettent de répondre à cette nouvelle question. L'OSCQ est une organisation qui regroupe les coordonnateurs en sécurité civile des ministères et organismes gouvernementaux québécois concernés par la mise en œuvre du Plan national de sécurité civile (PNSC) (Sécurité publique Québec, 2008).

Lors de ses travaux, l'OSCQ s'est interrogée sur le niveau de résilience des systèmes essentiels au Québec (OSCQ, 2008). Pour cela, elle a défini un glossaire de termes référant au risque en se basant sur nos travaux (Neault, 2009). De

manière plus spécifique, l'OSCQ utilise certains des termes que nous utilisons pour définir le risque : conséquence, dysfonction (défaillance), interdépendance (effets domino), ressource utilisée (dont la dégradation constitue un aléa).

En conséquence, seuls deux éléments, constitutifs de notre définition du risque à savoir les notions d'état et de vulnérabilité, ne semblent pas employés pour le moment. Toutefois, même si ces éléments ne sont pas définis nommément, ils sont pourtant utilisés. En effet, la démarche gouvernementale visant à accroître la résilience des systèmes essentiels au Québec se base sur la notion de résilience qui est définie comme « l'aptitude d'un système à maintenir ou à rétablir un niveau de fonctionnement acceptable malgré des défaillances » (OSCQ, 2008). Cette notion réfère directement à une acceptabilité de l'état dans lequel vont se trouver les composantes du système analysé. De ce fait, elle réfère en partie à la capacité d'un système à remplir sa mission même si certaines de ses composantes se trouvent en état de dysfonction. En effet, la défaillance est définie comme l'« état dans lequel un système ne peut plus remplir complètement ses objectifs » (OSCQ, 2008).

La notion de vulnérabilité est indissociable de la prise en compte de la variation d'état d'un système. Même si l'OSCQ ne semble pas utiliser ou caractériser la vulnérabilité d'un système, elle le fait indirectement. En effet, elle juge d'un état acceptable du système en fonction des conséquences engendrées et en considérant l'affectation possible du système par la perte des ressources qu'il utilise (OSCQ, 2008). Cette manière de procéder et une sorte de caractérisation de la vulnérabilité. Elle n'est pas tout à fait appréhendée comme nous le faisons mais elle est présente.

La définition du risque que nous proposons semble donc tout à fait acceptable, mais surtout utilisable d'un point de vue pratique. Elle a le mérite d'intégrer les notions (aléa, vulnérabilité, état, dysfonction, conséquence, effet domino) qui sont régulièrement employées quand il s'agit d'analyser et de gérer des risques.

Cependant, du travail reste à faire comme l'a montré l'exercice Domino effectué le 13 novembre 2008 à Québec par l'OSCQ (OSCQ, 2008). Cet exercice, effectué en présence d'une centaine de participants, a montré l'importance d'avoir une terminologie commune pour tous les participants. Il a également montré qu'il n'était pas aussi simple que cela de s'approprier une nouvelle terminologie.

6.2.2 L'organisation d'un système

Les quatrième et cinquième chapitres de ce travail présentent le mode d'organisation que nous proposons pour soutenir une analyse de vulnérabilité. L'étude est basée sur un système qui utilise et fournit des ressources. En fait, le fonctionnement du système dépend de l'utilisation de ressources qui proviennent de son environnement. Le système transforme ces ressources, en utilisant des fonctions et des infrastructures, de manière à fournir de nouvelles ressources dans son environnement. Ces ressources produites pourront être utilisées par un autre système.

L'utilisation d'un triplet ressources utilisées-système-ressources fournies semble très intéressante en raison de son applicabilité à décrire un contexte d'étude quel que soit le niveau d'analyse. En effet, cette représentation reste valide tant à un niveau macroscopique qu'à un niveau plus fin d'étude. Il fait penser en cela à une sorte de fractale. À un niveau global, le système peut être une infrastructure essentielle qui utilise et fournit des ressources. À un niveau moyen, le système devient une fonction qui utilise et fournit des ressources. À un niveau encore plus fin d'analyse, le système peut être un équipement qui lui aussi à des besoins et remplit une mission. Ce mode d'organisation et l'utilisation de notre définition du risque semblent donc particulièrement adaptés pour servir d'aide à la décision quel que soit le niveau de d'analyse. De ce fait, il est possible de dire que les concepts que nous proposons pourraient aider à mettre en œuvre le principe de subsidiarité qui est un des principes importants pour l'atteinte d'un développement durable.

Ce mode d'organisation semble relativement simple d'un point de vue théorique lorsque nous nous situons à un seul niveau d'analyse et que nous mettons de côté l'aspect fractal. Il est cependant possible de se demander s'il est adapté à la pratique et donc s'il peut être utilisé par les gestionnaires d'infrastructures essentielles.

À l'instar des questions portant sur la définition de nos concepts, des réponses à cette question ressortent des travaux effectués par le *Centre risque & performance.*

Les nombreux travaux de recherche effectués par le centre et plus spécifiquement les travaux de maîtrise montrent l'applicabilité des concepts de caractérisation d'un système dans son environnement tant dans un contexte de préparation aux situations d'urgence (De la lande de Calan, 2007 ; Hémond, 2008 ; Pageon, 2008) que dans celui de continuité opérationnelle des organisations (Guichardet, 2009 ; Khayate, 2008). Les applications développées dans ces mémoires montrent l'utilisation possible du triplet ressources utilisées-système-ressources fournies pour aborder la problématique de la gestion des risques appliquée aux infrastructures essentielles. De plus, ils montrent l'intérêt de cette formalisation dans un contexte d'analyse et d'évaluation des vulnérabilités d'un système.

Dans ses travaux, De la lande de Calan (2007) montre l'utilisation du triplet ressources utilisées-système-ressources fournies pour poser les bases d'une méthodologie de modélisation des interdépendances entre infrastructures essentielles de manière à identifier et anticiper les effets domino. Cette méthodologie propose de structurer les informations concernant les infrastructures essentielles de manière à ne garder que celles qui sont pertinentes pour la protection des infrastructures essentielles en regard de leur protection face aux défaillances en cascade.

Pour cette méthodologie, les infrastructures essentielles fournissent les informations nécessaires à la mise en place d'une base de connaissances faisant le

lien entre les ressources utilisées et l'impact sur l'état du système utilisateur lorsque ces ressources ne sont plus disponibles. L'état du système permet ensuite de déterminer si le système peut encore remplir sa mission (fournir une ressource). Il est ainsi possible de déterminer les conséquences, pour une ressource fournie, de la perte d'une ressource utilisée. À partir de cette base de connaissances, la méthodologie permet donc de modéliser les effets domino.

Les travaux de Hémond (2008), quant à eux, portent sur l'application de ces concepts à une infrastructure essentielle particulière à savoir le réseau routier faisant partie de l'infrastructure essentielle transport. La particularité du réseau routier provient de son utilisation. Une infrastructure essentielle utilise la ressource qui lui est acheminée par l'entremise du réseau routier, mais elle peut également utiliser le réseau routier pour réaliser différentes activités reliées à son fonctionnement, telles que l'entretien, la surveillance, la réparation ou l'accès à une infrastructure donnée. Une infrastructure essentielle utilise donc le réseau routier pour s'assurer que son système est fonctionnel et lui permettre de remplir sa mission.

Pour aborder cette problématique, la méthodologie proposée regroupe les utilisations possibles du réseau routier en deux grandes catégories, l'approvisionnement en ressources et les activités de support. Le réseau routier est donc à la fois considéré comme un élément pouvant affecter une ressource utilisée par une autre infrastructure essentielle et comme une ressource particulière. En considérant le réseau routier comme un facteur pouvant influer sur l'utilisation d'une ressource donnée, il s'agit donc de prendre en compte l'effet du réseau routier en termes de variation du délai d'approvisionnement ou d'accessibilité.

Les principes proposés par De la lande de Calan (2007) et par Hémond (2008) ont été complétés par les travaux de Guichardet (2009) qui proposent de structurer le système en ensembles fonctionnels permettant de mieux caractériser le mode

d'affectation de la variation d'états des ressources utilisées et des composantes du système sur les ressources fournies.

Chaque ensemble fonctionnel regroupe les infrastructures et fonctions nécessaires à la fourniture d'une ressource donnée. Aucune différenciation n'est vraiment effectuée entre les différentes composantes du système. Cependant, la méthode définit les informations devant être fournies par les experts des réseaux. Ces informations alimentent une base de connaissances qui permet de développer des modèles de dégradation des ressources fournies par le système. La méthode développée par Guichardet (2009) permet donc de caractériser la dégradation d'une ressource fournie due à la variation d'états des composantes d'un ensemble fonctionnel. Cette méthodologie met l'emphase sur la caractérisation de la phase de dysfonctionnement (état dégradé) du système en intégrant les modes de gestion normale et d'urgence existants de même que la possibilité d'utiliser des ressources alternatives.

Pageon (2008) va plus loin dans l'utilisation des notions de système et de ressources utilisées et fournies en proposant de définir les ressources essentielles pour le bien-être de la population. Pour cela, il propose de s'intéresser à la capacité des municipalités régionales de comté (MRC) à maintenir la fourniture des ressources essentielles à la population en utilisant une méthodologie d'approche par conséquences appliquée à l'analyse de risques et à l'évaluation des vulnérabilités.

De manière spécifique, cette méthodologie permet de démontrer l'importance d'intégrer les ressources essentielles lors de l'établissement d'un schéma de sécurité civile et par conséquent, de porter une attention particulière à la vulnérabilité des municipalités. Ainsi, lors de l'étape du traitement des risques, les municipalités peuvent prendre en compte les vulnérabilités présentes sur leur territoire.

Finalement, Khayate (2008) utilise également les concepts que nous proposons, mais cette fois-ci en les appliquant au domaine de la continuité des affaires et en considérant plus spécifiquement les fonctions d'un système. Il propose deux outils permettant de considérer des paramètres temporels, tels que la compressibilité d'une activité ou l'existence de dates jalons liées à une activité, mais aussi la dépendance des activités face aux ressources utilisées pour leur réalisation.

À un niveau opérationnel, le concept ressources utilisées-système-ressources fournies est donc applicable. De plus, il est largement accepté et utilisé par les partenaires industriels et gouvernementaux du *Centre risque & performance.* Qu'en est-il à un niveau stratégique ?

Les ateliers effectués par l'OSCQ, mais également par le Collège canadien de la gestion des urgences (CCGU) apportent une réponse à cette question.

Le Collège canadien de gestion des urgences a mis sur pied un cours de connaissance des infrastructures essentielles (CCGU, 2007a). Cette formation d'une journée permet de se familiariser avec le concept d'infrastructure essentielle, mais aussi de voir plus spécifiquement la problématique des interdépendances entre infrastructures essentielles. La prise en compte des interdépendances entre infrastructures essentielles s'effectue en étudiant les interactions entre les infrastructures essentielles et donc en se focalisant sur les liens et les échanges existants entre elles. L'analyse des interdépendances est directement basée sur l'organisation en triplet que nous proposons. De plus, l'organisation ressources utilisées-système-ressources fournies est également à la base d'ateliers plus spécifiques sur les interdépendances entre infrastructures essentielles qui sont dispensés par le collège canadien de gestion des urgences (CCGU, 2007b ; CCGU, 2008).

L'exercice de l'OSCQ sur la résilience des systèmes essentiels a directement montré l'application possible de l'organisation en triplet que nous proposons

(OSCQ, 2008). Pour améliorer cette résilience, l'OSCQ propose une approche méthodologique directement centrée sur les notions de systèmes, de ressources utilisées et fournies. Les participants à l'atelier ont largement reconnu l'importance d'utiliser ces concepts tant dans le domaine précis de la gestion des situations d'urgence que dans celui plus général de la mise en pratique du développement durable. Les travaux effectués ont entre autres permis une prise de conscience des interdépendances entre les systèmes de même que des besoins de ces derniers. La théorie a semblé difficile à intégrer au départ, mais par la suite un consensus est ressorti quant à l'importance d'utiliser ces notions et de passer rapidement à une phase d'opérationnalisation permettant d'intégrer ces concepts dans le mode de fonctionnement et de gestion des organismes et ministères provinciaux.

Dans l'organisation du système que nous proposons, nous ne considérons pas uniquement le système comme une entité figée. Nous proposons de regarder plus finement le mode d'organisation et de fonctionnement d'un système en analysant les infrastructures et les fonctions qu'il utilise pour remplir sa ou ses missions. Cette manière de procéder est déjà effectuée dans la pratique par les gestionnaires d'infrastructures essentielles. En effet, comme l'a montré Lapointe (2006), les infrastructures essentielles sont déjà analysées en termes de fonctions critiques et de fonctions de soutien de manière à se préparer adéquatement pour des situations d'urgence. Les travaux de l'ANL montrent également cette analyse fonctionnelle des infrastructures essentielles (Peerenboom and Fisher, 2007).

La dissociation du contexte d'étude en termes de système, composé de fonctions et d'infrastructures, de ressources utilisées et ressources fournies semble donc acceptée et appliquée par les spécialistes œuvrant dans les domaines des mesures d'urgence et de la continuité opérationnelle.

6.3 Application et opérationnalisation de la méthodologie proposée

Le troisième élément important de cette thèse, après les propositions d'une définition du risque et de l'organisation d'un système dans son environnement est

l'approche méthodologique proposée pour analyser la vulnérabilité d'un système. Le cinquième chapitre présente en détail cette approche.

De manière globale, nous pouvons en partie juger de l'applicabilité de notre méthodologie en nous basant sur les travaux réalisés par le *Centre risque & performance* et sur ceux effectués par l'OSCQ.

Les travaux de l'OSCQ confirment l'applicabilité, à un niveau stratégique, d'une méthodologie d'analyse des vulnérabilités basée sur le triplet ressources utilisées-système-ressources fournies. En effet, l'approche méthodologique proposée par l'OSCQ pour l'amélioration de la résilience des systèmes essentiels est directement basée sur les principes que nous proposons. Pour arriver à renforcer la résilience des systèmes essentiels au Québec, les étapes de la méthodologie de l'OSCQ consistent à :

- identifier les systèmes essentiels et les ressources essentielles qu'ils fournissent ;
- décomposer les systèmes essentiels en fonctions critiques ;
- caractériser les ressources essentielles utilisées.

Toutefois, l'approche de l'OSCQ est à ses premières phases de développement. Elle considère une variation d'état des ressources et des composantes des systèmes, mais elle ne pose pas encore de principes méthodologiques qui permettraient de relier les variations d'état des ressources avec celles du système.

Le guide méthodologique « Réduction de la vulnérabilité des infrastructures essentielles face à leurs interdépendances », proposé par le *Centre risque & performance* (Robert et Morabito, 2009), montre lui aussi qu'une approche déductive d'analyse des vulnérabilités est applicable à la gestion des risques en ce qui concerne le domaine spécifique des interdépendances entre infrastructures essentielles. Contrairement aux travaux de l'OSCQ, les travaux du *Centre risque & performance* ont permis de développer des outils, tels que les courbes de

dépendance, qui peuvent permettre de corréler les variations d'état de composantes reliées. Toutefois, ces travaux ne se penchent pas encore véritablement sur la caractérisation de l'état du système ou sur la dépendance du système face à l'utilisation des données ou des informations.

L'approche générale de la méthodologie proposée est donc applicable et appliquée dans la pratique. Cependant, il est possible de se demander si les étapes spécifiques que nous proposons pour analyser les vulnérabilités d'un système sont applicables. De plus, est-ce que les principes proposés pour caractériser le système et ses dépendances face à l'utilisation des données sont applicables ?

Pour répondre à ces questions, il faut regarder les étapes de caractérisation de la méthodologie proposée pour voir si elles sont utilisables dans la pratique.

6.3.1 La caractérisation de l'environnement

Cette étape de la méthodologie est véritablement l'étape qui, pour le moment, a montré son applicabilité dans la pratique. En effet, les travaux du *Centre risque & performance* se sont concentrés ces dernières années sur l'analyse des interdépendances entre infrastructures essentielles. Le fait de différencier l'environnement en secteurs en utilisant les principes de la cartographie souple est déjà appliqué avec succès pour les villes de Montréal et de Québec (Robert et coll., 2007 ; Robert and Morabito, 2008 ; Robert et coll., 2008). La segmentation est parfaitement adaptée à l'étude des interdépendances reliées à des liens physiques. Elle peut être plus complexe pour les autres types de liens (géographique, cybernétique et logique).

Le fait de segmenter le secteur d'étude, en utilisant le concept de la cartographie souple, présente de nombreux avantages, tel que de faciliter l'échange d'information entre les acteurs des mesures d'urgence (utilisation de numéro pour chaque secteur définis). Elle permet également une localisation géographique plus précise (secteurs orientés suivant le nord). Toutefois, l'avantage principal de ce

mode de sectorisation est la possibilité de localiser plus ou moins précisément les différentes composantes des infrastructures essentielles. Cette possibilité permet de gérer un niveau de vulnérabilité acceptable en termes de terrorisme face à la localisation des infrastructures. Cependant, plus la localisation est précise, plus l'information est pertinente pour être utilisée dans un processus de gestion des risques.

Ce mode de sectorisation même s'il est très utile pour les dépendances et interdépendances directes entre infrastructures essentielles n'est pas forcément adéquat pour les interdépendances géographiques. En effet, cette sectorisation ne tient pas compte des caractéristiques physiques et sociologiques de l'environnement du système. Par exemple, pour un secteur donné, la topographie, qui est importante pour l'écoulement d'une matière, telle que de l'eau, peut être variable.

Il faut donc sectoriser l'environnement du système en considérant à la fois ses caractéristiques propres, mais également ses relations avec le système pouvant l'impacter. Pour cela, il est possible d'utiliser une technique de superposition cartographique. Chaque caractéristique étant matérialisée par une couche donnée.

Il est évident que le nombre de critères permettant de caractériser la zone d'étude dépend de l'objectif de l'analyse, du niveau de raffinement recherché, mais également du type de conséquences caractérisé.

Une des premières segmentations à effectuer consiste à diviser la zone d'étude (environnement) en secteurs ayant des caractéristiques similaires en termes de fourniture de ressources. En effet, la dégradation de l'état de la ressource ou des ressources fournies par un système (dysfonction du système) va potentiellement engendrer des conséquences sur l'environnement. Il faut donc nécessairement connaître où vont se faire ressentir ces dysfonctions. Contrairement à d'autres modes de sectorisation, il est évident que les secteurs ainsi déterminés n'auront pas

forcément des superficies et des formes identiques. Mais cette information est indispensable, car la notion de ressource est à la base de la caractérisation des interdépendances entre infrastructures essentielles.

Le deuxième critère à prendre en compte consiste à déterminer les éléments importants présents dans l'environnement du système qui pourraient utiliser la ressource fournie par le système analysé. Il s'agit donc de définir les éléments valorisés de l'environnement qui se trouvent dans les secteurs définis et donc dans la sphère d'influence du système. Les éléments valorisés de l'environnement regroupent tous les éléments qui peuvent avoir une importance particulière pour les objectifs de l'analyse. Il est évident que les éléments importants dans le cadre de la caractérisation des interdépendances entre infrastructures essentielles sont les infrastructures essentielles elles-mêmes.

En combinant différentes couches d'information permettant de caractériser l'environnement, il est possible de définir des secteurs plus précis. Les secteurs ainsi définis permettront une véritable gestion proactive des risques et des vulnérabilités.

Cependant, la combinaison des informations disponibles pose un problème de taille : la gestion de la confidentialité. Ce mode de traitement de l'information conduit presque inévitablement à une localisation très précise des infrastructures composant les systèmes.

Plus les secteurs définis auront des petites superficies, plus l'information sera précise. En raffinant la taille des secteurs, nous obtenons une information plus facilement exploitable en termes de continuité opérationnelle ou en termes de mesures d'urgence. Cependant, nous arrivons également à localiser de manière plus précise les différentes composantes des systèmes présents dans un environnement donné. Cela peut être un inconvénient si cette information traitée tombe entre de

mauvaises mains. C'est pourquoi cette information ne devrait être disponible que pour les gestionnaires de mesures d'urgence.

Nous nous retrouvons donc devant un paradoxe. Plus une information est précise (ici la localisation d'une infrastructure essentielle), plus elle rend le système vulnérable à un acte de malveillance. Toutefois, plus une information est précise et plus la gestion des vulnérabilités en termes d'interdépendances entre systèmes sera efficace. Il n'est pas simple de régler ce paradoxe. Cela ne peut se faire qu'en signant des ententes entre gestionnaires de systèmes et en prévoyant des mises en commun des informations selon des protocoles très précis. C'est pour cela que l'ensemble des travaux sur les interdépendances entre infrastructures essentielles débute invariablement par le développement d'un cadre précis pour l'échange des informations.

De toute façon, de manière ultime, ce paradoxe entre le fait d'avoir de l'information, de la traiter, de la gérer correctement et le fait de ne pas vouloir qu'elle se retrouve entre de mauvaises mains est indissociable de la gestion des risques. Il est vrai qu'elle apparaît peut-être plus complexe quand il s'agit d'analyser les vulnérabilités d'un système. Ceci est d'autant plus vrai qu'actuellement, le contexte mondial met la préoccupation terroriste à l'avant-scène.

Le deuxième outil permettant de caractériser l'environnement est la création de courbes de dépendance. Cet outil est également utilisé avec succès par le *Centre risque & performance* (Robert et Morabito, 2009). En fait, les courbes de dépendances permettent plus exactement de gérer les relations de dépendance entre les systèmes. Elles sont particulièrement intéressantes dans leur capacité à intégrer la composante temporelle dont la considération est indispensable pour gérer le risque et plus spécifiquement sa composante vulnérabilité.

Toutefois, la problématique demeure la même que pour la sectorisation de l'environnement. Les courbes de dépendance sont un moyen de traiter de l'information de manière à la rendre utilisable pour se préparer aux situations d'urgence voir pour les prévenir. Le traitement des données fournies par les gestionnaires de systèmes induit forcément l'identification de vulnérabilités. C'est le but de la méthodologie proposée. Cependant, l'identification de nouvelles vulnérabilités induit un certain stress en pensant que des personnes malintentionnées puissent les connaître ou les découvrir. Cette problématique est véritablement un élément prépondérant à considérer pour une bonne gestion des risques. C'est là toute la difficulté d'une communication efficace des risques.

Les outils que nous proposons (sectorisation et courbes de dépendance) sont déjà utilisés en pratique. La sectorisation de l'environnement que nous proposons ne devrait donc pas poser de problème majeur. Seul l'élément de la communication et de l'utilisation d'information pouvant être jugée sensible pourrait s'avérer problématique. Cependant, une bonne définition du contexte d'étude (cadre et limite de l'étude) associée à un cadre d'échange d'information bien défini devrait permettre de régler ce problème.

6.3.2 La caractérisation du système

Dans le contexte des travaux du *Centre risque & performance*, cette caractérisation n'est encore que peu abordée à un niveau pratique. Comme nous l'avons vu, le principe d'analyser le système en termes de fonctions et d'infrastructures est généralement admis et réalisé en pratique (Lapointe, 2006 ; Peerenboom and Fisher, 2007). Toutefois, le principe de combiner les états des composantes constitutives du système de manière à analyser la répercussion de leurs variations sur l'état des ressources fournies n'est pas encore mis en pratique. Les travaux actuels visent plus à subdiviser le système en ensembles fonctionnels, regroupant certaines composantes du système (infrastructures et fonctions), qui permettent de caractériser la variation d'état des ressources fournies (Guichardet, 2009).

Toutefois, il est toujours possible de se demander si la caractérisation du système, telle que nous la proposons est applicable en pratique ? Il n'est pas simple de répondre à cette question.

Les deux premiers principes consistant à utiliser une analyse fonctionnelle et un organigramme technique pour identifier les composantes importantes d'un système ne semblent pas problématiques à appliquer en pratique. En effet, ces concepts sont déjà largement utilisés dans le domaine industriel et plus particulièrement dans celui de la gestion de projet. De plus, Lapointe (2006) et l'OSCQ (2008) montrent que le besoin d'identifier les composantes importantes d'un système n'est pas remis en question.

Le troisième principe à la base de la phase de la caractérisation du système que nous proposons consiste à déterminer les états possibles des composantes importantes du système. Ce principe ne semble pas non plus remis en question. Il peut être plus problématique à appliquer en particulier en ce qui a trait à la définition des critères à utiliser pour établir les seuils de variation d'états. Toutefois, ce principe ne devrait pas être trop problématique à mettre en œuvre, et cela, pour deux raisons principales :

- la variation d'état d'une fonction ou d'une infrastructure est généralement définie dès l'étape de conception d'un système. En effet, si nous prenons le cas d'une infrastructure, sa durée de vie utile est définie. Il est possible d'en tirer une courbe indiquant une variation d'états comme nous l'avons montré au chapitre 3.
- la démarche pour définir des états possibles que ce soit pour une composante d'un système ou pour une ressource fournie demeure la même. Cette démarche qui se base sur le jugement d'experts, a fait ces preuves pour la caractérisation de l'environnement et ne devrait donc pas poser de problème pour la caractérisation du système.

Le quatrième et dernier principe est la combinaison des états. Pour cela, nous proposons l'utilisation des concepts à la base des arbres de fonctionnement et de la logique floue. Nous avons également proposé des critères d'agrégation relativement simples. Les techniques d'analyse des risques basées sur les arbres sont bien connues et souvent utilisées dans le domaine industriel. Le seul changement que nous apportons à ces méthodes d'analyse est la manière d'analyser la succession des portes logiques utilisées. La seule difficulté qui pourrait ressortir pour appliquer la caractérisation du système est l'utilisation de la logique floue. Toutefois, comme nous l'avons précisé, nous proposons l'utilisation des concepts à la base de la logique floue et non le développement de calculs complexes. De plus, l'utilisation de la logique floue n'a d'intérêt que dans un contexte d'analyse des vulnérabilités très précises. Il paraît plus important d'initier un processus de caractérisation du système.

Dans cette étape de caractérisation du système, seule l'utilisation de la logique floue pourrait rebuter certaines personnes qui la jugeraient trop complexe. Toutefois, ces principes ne seraient utilisés que pour une analyse plus fine des vulnérabilités. De ce fait, il ne semble pas que cette étape présenterait des difficultés majeures lors d'une application pratique.

6.3.3 La caractérisation des besoins du système

L'étape de caractérisation des besoins du système est également une étape qui a démontré son applicabilité grâce aux travaux réalisés par le *Centre risque & performance* (Robert et Morabito, 2009). La caractérisation des besoins du système peut se faire suivant une approche similaire à celle utilisée pour caractériser l'environnement. En effet, dans un cas, il s'agit de définir la dépendance de l'environnement face aux ressources fournies par le système alors que, dans l'autre cas, il s'agit de définir la dépendance du système face aux ressources présentes dans l'environnement. Les difficultés de mise en œuvre de la caractérisation des besoins du système sont donc similaires à celles rencontrées pour la caractérisation de l'environnement.

Toutefois, la particularité de la méthodologie que nous proposons est qu'elle se focalise sur la dépendance du système face à l'élément cybernétique et plus spécifiquement face aux données et aux informations. Pour cela, nous proposons de considérer la cybernétique dans son sens premier en nous focalisant sur la problématique de sûreté de fonctionnement et en utilisant les principes de l'endorsement.

La première question que nous pouvons nous poser est de se demander si les intervenants dans le domaine de la gestion des risques ou dans celui des technologies de l'information seraient intéressés par une telle approche.

La réponse à cette question est sans aucun doute positive. L'Union internationale des communications insiste sur la nécessité de considérer à la fois la qualité de fonctionnement et la qualité de service (UIT-T, 2005). L'approche que nous proposons en nous focalisant sur les variations d'états des informations et leur répercussion sur l'état des composantes d'un système permet de considérer ces deux éléments d'une qualité globale. Les présentations que nous avons effectuées lors du premier symposium international sur la gestion des risques et la cyberinformatique (Petit et Robert, 2004) et lors du symposium national sur les télécommunications d'urgence (Petit et Robert, 2007), nous ont également montrées l'intérêt des spécialistes en gestion des risques reliés aux technologies de l'information pour la problématique des vulnérabilités cybernétiques et pour l'approche que nous proposons.

La deuxième question que nous pouvons nous poser est de se demander si les principes que nous proposons pourraient être facilement applicables à un cas pratique.

Il est difficile dans l'état actuel de nos travaux de répondre de manière indiscutable à cette question. L'utilisation des principes de l'endorsement ne devrait pas poser

de problème si ce n'est qu'il faudra définir avec précision l'événement qui sera considéré et les différentes conditions pouvant mener à sa réalisation. La difficulté principale d'application de cette partie de la méthodologie à un cas concret résulte sans aucun doute dans le nombre de critères qui seront utilisés pour évaluer l'état des données.

6.4 Les travaux futurs

Les concepts posés ne constituent pas une fin en soi. Il reste des choses à faire notamment pour les opérationnaliser, en particulier en ce qui a trait à la caractérisation des besoins du système. La prise en compte de la cybernétique devrait être raffinée. En effet, les principes de l'endorsement et la définition de conditions, pouvant affecter le système, sont prometteuses et applicables. Cependant, il faut mieux connaître l'organisation des systèmes et mieux comprendre leur dépendance face à l'utilisation des données et de l'information en général. Nous avons présenté un ensemble de critères pouvant être utilisés. Cependant, il reste véritablement à préciser ceux qui sont indispensables pour pouvoir caractériser correctement la dépendance du système. Il est évident que les notions d'importance des données, d'état des données et de temps durant lequel le système peut s'en passer sont les critères minimaux à considérer. Cependant, d'autres critères, tels que le type de données ou leur mode de transfert, pourraient être pris en compte pour effectuer une bonne évaluation de la dépendance cybernétique des systèmes. La définition des critères à considérer ne peut véritablement se faire qu'en partenariat avec les gestionnaires de système. De plus, il est assuré que ces critères vont varier suivant le système, mais également suivant les fonctions du système considérées.

Un autre élément à raffiner, concernant la caractérisation des besoins du système, est le mode de combinaison des conditions définies. En effet, il est évident que plusieurs conditions peuvent mener au même résultat en ce qui a trait à la dégradation de l'état fonctionnel du système. Par exemple, un retard dans l'obtention d'une donnée peut affecter le système de la même manière qu'une

donnée dégradée obtenue dans des délais raisonnables. Toutefois, les deux éléments combinés, retard et dégradation, peuvent se traduire par un autre mode d'affectation du système. Ce sont ces modes d'agrégation des conditions d'endorsement qu'il faut raffiner. L'endorsement permet ce raffinement en intégrant dans les conditions nécessaires des combinaisons de conditions supportives. Plus exactement, il convient de définir des conditions adaptées à une réalité plus complexe en combinant plusieurs critères permettant de caractériser les données, mais également leurs modes d'affectation des systèmes. Le concept de l'endorsement peut également être raffiné en essayant de déterminer le niveau de certitude existant par rapport à la possibilité de réalisation d'une condition donnée. Comme le propose Robert (1989), ce niveau de certitude quant à l'existence d'une condition peut être évalué suivant quatre niveaux (Très sûr, sûr, peu sûr, impossible).

Par contre, la prise en compte d'un niveau de certitude pour l'existence d'une condition n'est pas vraiment utile tout de suite. Le fait de définir correctement des conditions pouvant mener à l'affectation du système est suffisant au départ. La prise en compte de possibilité d'apparition des conditions pourra être utile lorsque les systèmes et leur dépendance face à l'utilisation de données seront bien connus.

En ce qui a trait à l'ensemble des étapes de caractérisation, il existe un autre élément qu'il faut absolument considérer et que nous n'avons pas encore intégré à nos concepts. Il s'agit de la prise en compte du facteur humain et, plus exactement, de la fiabilité humaine. Cet élément est prépondérant pour le fonctionnement de tout système et ceci d'autant plus pour l'analyse de la cybernétique. En effet, les systèmes sont automatisés en partie pour palier à la défaillance des humains les opérant. Par contre, lorsque le système informatique entre en dysfonction, ce sont les humains qui doivent reprendre en main le système. Ceci est paradoxal. Il est demandé à un humain de récupérer les dysfonctions d'un système informatique qui est mis en place car il est jugé plus fiable que l'être humain. Dans un contexte de

fiabilité globale, il faut donc combiner à l'analyse de la vulnérabilité des systèmes, face à la cybernétique, la prise en compte de la fiabilité humaine.

Cet élément humain peut être intégré de deux manières à la méthodologie proposée. Il est possible d'analyser la dépendance du système face à la ressource humaine. De cette manière, l'humain est considéré comme une ressource essentielle pour le fonctionnement du système au même titre que la cybernétique. La deuxième manière de considérer le facteur humain est de l'intégrer comme un moyen de protection ou comme un élément à combiner avec l'élément cybernétique. De cette manière, l'élément humain peut être intégré comme un critère de caractérisation de l'affectation du système par les données. En ce sens, il constitue un moyen de détection et de récupération de la dysfonction du système.

Les principes méthodologiques proposés doivent aussi mieux intégrer la notion de résilience du système. Cette notion est déjà considérée par la détermination d'un état dégradé de fonctionnement du système. Cet état correspond tout à fait à la partie de la résilience qui correspond à la capacité d'un système à remplir sa mission même s'il n'est pas dans un état optimal. Il faut intégrer la deuxième partie du concept de résilience à savoir la capacité d'un système à revenir à un état de fonctionnement optimal ou normal (état du système prévalant avant la dégradation). Cette deuxième manière de voir la résilience est un peu plus complexe à considérer dans le sens où elle doit intégrer l'adaptabilité du système à son environnement et sa capacité à trouver un nouvel état d'équilibre. Ce nouvel état devrait en effet constituer le nouvel état optimal de fonctionnement. De plus, une meilleure connaissance des informations indispensables au fonctionnement du système permettra de le rendre plus résilient. En effet, un système peut-il être résilient sans information ou avec de mauvaises informations ? La réponse à cette question est évidemment négative. Il faut donc déterminer un niveau de fonctionnement minimal acceptable, le niveau de résilience acceptable du système analysé.

Il faut également prendre en compte, dans la caractérisation des besoins du système, les autres types de ressources qui sont indispensables à son fonctionnement. Les principes de l'endorsement, tel que nous l'avons défini, pourraient être utiles pour caractériser la manière dont la dégradation de ces ressources pourrait affecter le système.

Finalement, la cybernétique, le facteur humain et la prise en compte de la résilience du système devraient être abordés plus finement pour soutenir adéquatement la mise en œuvre de systèmes d'alerte précoce (*Early Warning Systems*) qui permettront de développer des moyens plus efficaces de réponse aux défaillances d'un système. Ils permettront également de mettre en œuvre des systèmes de communication et d'échange d'information plus adaptés. Les concepts supportant la méthodologie proposée pourraient déjà constituer une bonne base pour la mise en place des systèmes de veille.

6.5 Conclusion

Le but principal de ce travail semble atteint dans le sens où il a permis de redéfinir des concepts, de proposer des définitions et de poser les bases et les principes permettant de sous-tendre une méthodologie déductive d'analyse des vulnérabilités. Les hypothèses posées pour encadrer ce travail ont été vérifiées grâce à l'atteinte des objectifs spécifiques.

Le fait que nous posons des principes de caractérisation et proposons des moyens pour évaluer les vulnérabilités cybernétiques d'un système sans imposer d'outils à utiliser est une force de notre méthodologie. Le seul impératif est de suivre la démarche et les principes proposés en utilisant au mieux le niveau d'information disponible. L'intégration de l'expertise des gestionnaires et des opérateurs des systèmes est indispensable.

Une autre force de notre méthodologie est le fait qu'elle permet de prendre en considération les trois composantes de la vulnérabilité (amont, interne et aval). Elle

permet donc de caractériser la vulnérabilité globale reliée à un système. De plus, les étapes de caractérisation peuvent être appliquées indépendamment les unes des autres. De cette manière, cette méthodologie peut permettre de se focaliser sur une composante particulière de la vulnérabilité et donc sur un élément précis du système (ses composantes ou ses interfaces avec l'environnement).

L'application concrète de l'approche méthodologique proposée peut être confrontée à quelques difficultés en ce qui a trait en particulier à la gestion de la confidentialité des données. D'autre part, plus l'objectif de l'utilisation de cette approche sera d'obtenir une analyse fine des vulnérabilités reliées à un système et plus cette méthodologie pourra être lourde à employer. En effet, l'utilisation poussée des outils proposés (arbres, logique floue et endorsement) et la multiplication des critères d'analyse pourraient rendre complexe l'application de la méthodologie.

Toutefois, une application moins poussée des concepts proposés pourrait permettre une gestion proactive des risques. Il pourrait être suffisant, à tout le moins dans une première approche, de ne pas utiliser la logique floue et de limiter le nombre de critères pris en compte. Cela permettrait d'initier le processus et de développer une première génération de courbes de dépendance qui permettraient de déterminer les marges de manœuvre disponible pour gérer le système et anticiper les situations d'urgence. Par la suite, l'étape de suivi permettrait, dans un deuxième temps, de raffiner les courbes de dépendance en utilisant plus de critères et les concepts de la logique floue.

Il faut garder à l'esprit qu'il ne s'agit pas de définir un processus infaillible dont les résultats seraient indiscutables et qui lèverait toute incertitude. Il est indéniable que plus l'analyse sera fine et précise et plus la gestion des vulnérabilités sera efficace. Toutefois, les étapes de caractérisation proposées pourront être couplées à un outil de veille de façon à permettre la mise en œuvre de moyen d'alerte efficace. En fait, la méthodologie proposée demeure un outil d'aide à la décision. Elle ne constitue

en aucun cas un processus de décision en tant que tel qui devrait se substituer aux gestionnaires d'infrastructures essentielles.

La méthodologie proposée de même que les concepts sur lesquels elle repose peuvent encore être améliorés notamment en raffinant les concepts d'endorsement et la définition des conditions permettant d'anticiper l'affectation d'une fonction du système. Il reste donc des choses à faire pour bonifier la méthodologie proposée en intégrant entre autres la prise en compte de la fiabilité humaine mais aussi la dépendance du système face à des ressources autres que cybernétiques.

CONCLUSION

Les infrastructures essentielles ou infrastructures critiques jouent un rôle primordial tant au niveau du développement économique que du développement social de la société civile. Ces systèmes complexes deviennent de plus en plus indispensables au bon fonctionnement des sociétés actuelles. Elles sont spécifiquement développées pour répondre aux besoins des populations. C'est d'ailleurs pour cela que certains auteurs n'hésitent pas à qualifier ces infrastructures essentielles de réseaux de support à la vie (Brunsdon, Daly and Lamb, 2003 ; Robert, 2008 ; Guichardet, 2009). Cela ne veut pas dire que, sans ces systèmes, la vie ne serait pas possible, mais cela souligne la croissance de la dépendance de la société civile face aux éléments fournis par ces infrastructures essentielles.

La crise financière qui sévit actuellement au niveau mondial est un parfait exemple de notre dépendance face au bon fonctionnement des infrastructures essentielles. Cette crise a comme origine l'effondrement du marché immobilier américain du fait des difficultés rencontrées par les ménages à faible revenu ou de la classe moyenne pour rembourser les crédits à risque (*subprimes*) qui leur avaient été consentis pour l'achat de leur logement (LesEchos, 2008).

Ce phénomène d'endettement des ménages américains a pu survenir entre autres du fait de taux d'intérêts très bas pratiqués par la Banque centrale des États-Unis suite à la crise boursière sur les valeurs Internet (Bulle Internet) en 2000 et les attentats du 11 septembre 2001 (LeMonde, 2008). Ces mécanismes économiques avaient pour but de stimuler la consommation pour favoriser la croissance des États-Unis.

En juin 2007, les premiers signes qu'une crise financière importante se développe apparaissent avec la fermeture de fonds d'investissement par Bear Searns. Les événements se sont enchainés jusqu'à la faillite de Lehman Brothers en septembre 2008 (LesEchos, 2008). Les États, pour essayer d'éviter une crise économique, ont racheté des banques et ont adopté des plans de plusieurs centaines de milliards de dollars pour racheter des créances contractées par ces mêmes banques. Toutefois, la

crise financière s'est progressivement transformée en crise économique entrainant l'entrée en récession de nombreux pays, tel que le Japon, 2e économie mondiale, en novembre 2008 (LeTemps, 2008).

Une crise, au départ immobilière, s'est donc transformée en crise financière en raison du mode de fonctionnement des systèmes bancaires, mais également du fait de la dépendance de la société civile face aux infrastructures essentielles du domaine des finances. Cette crise tend maintenant à se transformer en crise économique affectant en cela notre mode de développement.

La dépendance de la société face aux infrastructures essentielles financières est flagrante puisque nous assistons actuellement à un dysfonctionnement majeur de ces organismes qui se répercute sur les infrastructures essentielles de production manufacturière et industrielle, telle que l'industrie automobile, et sur l'ensemble des autres infrastructures essentielles par l'entremise des liens logiques. Toutefois, le même constat est certainement valide pour les autres secteurs des infrastructures essentielles. Il n'est pas utile d'attendre une défaillance majeure de ces systèmes pour se préparer à réagir de manière adéquate en cas de problème. Cette préparation ne devrait pas incomber uniquement aux seuls gestionnaires d'infrastructures essentielles. Ces systèmes complexes sont indispensables actuellement, mais ils le seront certainement encore plus dans les années futures. Il est impossible de penser qu'un retour en arrière soit possible et même souhaitable.

Pour favoriser un développement durable, il faut donc s'assurer de la fiabilité de ces systèmes. Pour cela, il faut favoriser la mise en œuvre d'une gestion proactive des risques qui permettra d'anticiper les dysfonctionnements possibles de ces systèmes de manière à pouvoir se préparer et réagir le plus rapidement et le mieux possible.

Un autre élément, qui doit être pris en compte, est la dépendance des infrastructures essentielles et donc de la société en générale à l'utilisation des communications et

de l'outil informatique. En effet, les systèmes supportant notre développement sont de plus en plus complexes et interconnectés nécessitant pour leur gestion l'échange d'une quantité importante de données. Ce phénomène est amplifié par l'automatisation croissante de ces systèmes. Cette dépendance à la cybernétique se doit donc d'être abordée.

Depuis les dix dernières années, de nombreux travaux abordant les risques associés aux infrastructures essentielles se développent en réaction à une prise de conscience mondiale de l'importance de ces systèmes pour notre qualité de vie. Ces travaux ont principalement été initiés suite à la succession des événements terroristes survenus au début des années 2000 aux États-Unis et en Europe. L'élément cybernétique commence à être considéré dans ces travaux en réaction à des attaques informatiques visant spécifiquement ces systèmes complexes. Il suffit de penser aux attaques ayant visé les sites Internet de la Géorgie en août 2008 (LeDroit, 2008). De ce fait, les travaux d'analyses des risques associés aux infrastructures essentielles abordent principalement la problématique des risques sous l'angle de la sécurité en privilégiant une approche classique des risques axée sur la prise en compte des aléas et des conséquences. Les différents États de la planète se préparent même à réagir à une cyberguerre (Trudel, 2008).

Parallèlement à ces approches relativement classiques des risques, une autre tendance d'analyse privilégiant l'étude des vulnérabilités tend à se développer. Cette nouvelle tendance vise un renforcement des systèmes de manière à pouvoir améliorer leur résilience. Elle correspond en cela véritablement au développement d'une gestion proactive des risques.

Mais qu'est-ce que le risque, la vulnérabilité ou même la résilience ?

Il est parfois un peu difficile de faire la différence entre ces termes et véritablement savoir à quoi ils réfèrent. De manière classique, les notions de vulnérabilité et de risque sont souvent confondues. La résilience peut également avoir diverses

significations suivant les personnes qui l'emploient. Toutefois, s'il est possible de parler de risque de manière générale, il est plus difficile de parler de résilience et de vulnérabilité sans définir sur quoi elles portent. Ces deux notions sont indissociables du système auquel elles réfèrent et plus spécifiquement de la variation de l'état de ce système.

Pour lever cette ambigüité face aux concepts de risque, vulnérabilité et résilience, nous avons proposé notre propre définition du risque qui intègre les notions d'aléas, de vulnérabilité, d'état du système, de dysfonction, de conséquence et d'effet domino. La combinaison de ces six éléments permet véritablement de permettre d'aborder le risque dans sa globalité. L'état du système et la vulnérabilité se retrouvent au cœur du risque. La notion d'état du système et la prise en compte de ses possibilités de variation permettent également d'introduire les notions de résilience et de marge de manœuvre. Ces deux derniers éléments sont indispensables pour une gestion proactive des risques qui permettra d'améliorer les processus de continuité opérationnelle et de mesures d'urgence.

Les définitions du risque et de ses éléments associés étant définies, nous avons proposé les concepts de base qui permettent de soutenir une approche méthodologique d'analyse des vulnérabilités d'une infrastructure essentielle.

Cette approche est une approche déductive qui, en partant d'un niveau de conséquences acceptables et en remontant vers les aléas pouvant engendrer ces conséquences, vise à analyser les différents types de vulnérabilité (aval, interne et amont). Chacun de ces types de vulnérabilité est abordé par une étape de caractérisation spécifique :

- la caractérisation de l'environnement du système permet d'analyser la vulnérabilité aval en se focalisant sur la répercussion de la dégradation de la ressource fournie par le système sur son environnement ;

- la caractérisation du système permet d'analyser la vulnérabilité interne du système en se focalisant sur son mode d'organisation structurelle et fonctionnelle ;
- la caractérisation des besoins du système permet d'analyser le dernier type de vulnérabilité à savoir la vulnérabilité amont en se focalisant sur la variation d'état des ressources nécessaires au fonctionnement du système.

De manière à intégrer également la prise en compte de la vulnérabilité cybernétique des infrastructures essentielles, la caractérisation des besoins du système se focalise plus spécifiquement sur les notions de qualité de fonctionnement et de qualité de service reliées à l'utilisation de données.

L'approche méthodologique proposée prend en compte les relations existantes tant entre les différentes composantes d'un système (infrastructure essentielle) qu'entre ce système et son environnement. Pour cela, elle propose des moyens, basés sur une échelle d'état à trois niveaux (normal, défaillant et hors service), qui pourraient permettre d'analyser l'évolution temporelle du système dans son environnement. Cette prise en compte de différents niveaux d'états et de la composante temps devrait également permettre de définir un niveau de résilience du système de même que les marges de manœuvre dont disposent les gestionnaires d'infrastructures essentielles avant de devoir mettre en œuvre des mesures particulières de gestion.

La méthodologie proposée demeure en grande partie à un niveau conceptuel bien que de nombreux concepts sur lesquels elle se base ont fait leur preuve dans la pratique. Ils restent d'importants défis à relever de manière à pouvoir opérationnaliser cette approche. L'un de ces défis, qui est d'autant plus prépondérant que cette approche se focalise sur le mode de fonctionnement des infrastructures essentielles et leur dépendance face à l'outil cybernétique, est la gestion de la confidentialité des informations. Toutefois, cette problématique est intrinsèque à la gestion des risques. Il faut de l'information pour gérer les risques,

mais produire et traiter cette information peut générer de nouvelles vulnérabilités et donc d'autres risques.

L'approche proposée n'est pas une fin en soi. Elle ne constitue en aucun cas la panacée renvoyant la solution ultime qui permettrait de gérer l'ensemble des risques associés au fonctionnement des infrastructures essentielles.

Elle se veut plus un complément aux méthodes actuelles abordant plus spécifiquement la sécurité des infrastructures essentielles en intégrant une approche de sûreté de fonctionnement. Elle permet en cela d'aborder la problématique des risques cybernétiques en ne se focalisant pas uniquement sur la sécurité et en considérant la problématique de l'intégrité des données et de la dépendance des infrastructures essentielles à l'utilisation de ces données.

La méthodologie que nous proposons répond donc au constat fait par la *Commission on Cybersecurity for the 44th Presidency* (CSIS) qui souligne le besoin d'avoir une approche intégrant à la fois la confidentialité et la disponibilité des données, mais également l'intégrité de ces données (CSIS, 2008).

Il est cependant évident qu'il demeure des choses à effectuer pour raffiner nos concepts notamment en ce qui a trait à la détermination des conditions supportant l'endorsement, mais également aux moyens de combiner ces conditions. Les autres dépendances des infrastructures essentielles doivent être intégrées en considérant les ressources utilisées autres que cybernétiques. Il faudra également intégrer la prise en compte de la fiabilité humaine. Il convient en fait de raffiner les concepts et la méthodologie de manière à favoriser une gestion plus proactive des risques, mais surtout de supporter des systèmes d'alerte précoce et de communications des risques. Les travaux futurs devront permettre l'atteinte d'une approche méthodologique la plus complète possible de manière à supporter le plus adéquatement possible les prises de décisions des gestionnaires d'infrastructures essentielles.

Il reste donc encore beaucoup de chemin à parcourir pour améliorer la résilience des systèmes complexes que constituent les infrastructures essentielles. Ce chemin risque d'être long et sinueux, mais nous pensons que l'approche méthodologique proposée constitue un pas dans la bonne direction pour améliorer le niveau de résilience des infrastructures essentielles et de la société civile. Elle devrait donc contribuer à l'atteinte d'un développement plus durable.

RÉFÉRENCES

AGENCE NATIONALE DE LA RECHERCHE (2008). Concepts systèmes et outils pour la sécurité globale, appel à projets 2008. Agence Nationale de la Recherche, Université de Technologie de Troyes, France, 24 p.

ANDRÉ, P., DELISLE, C. E., et REVÉRET, J.-P. (2003). L'évaluation des impacts sur l'environnement, deuxième édition : Processus, acteurs et pratique pour un développement durable. Presses internationales Polytechnique, Montréal, Québec, Canada, 519 p.

ANL (2008). Infrastructure Assurance Center. Site Internet de l'Argonne National Laboratory [En ligne], États-Unis.
http://www.dis.anl.gov/exp/ia/index.html (Consulté le 31 juillet 2008).

AUFFREY, C. (2008). Les infrastructures critiques des états vulnérables. JDN Solutions. Site Internet du Journal du net [En ligne], France.
http://www.journaldunet.com/solutions/securite/analyses/08/0218-systemes-scada-energie.shtml (Consulté le 1 août 2008).

BARPI (2008). L'accident de Seveso : rejet à l'atmosphère de dioxines dans une usine chimique. Base de donnée ARIA, Enseignements tirés des accidents technologiques, Bureau d'Analyse des Risques et Pollutions industrielles, ministère de l'Écologie, du Développement et de l'Aménagement durable, France, ARIA No 5620, 8 p.

BBC NEWS (2008). London attacks, special report. Site Internet de la British Broadcasting Corporation [En ligne], Grande-Bretagne.
http://news.bbc.co.uk/1/hi/in_depth/uk/2005/london_explosions/default.stm
(Consulté le 31 juillet 2008).

BERNARD, J. G., AUBERT, B. A., BOURDEAU, S., CLÉMENT, É., DEBUISSY, C., DUMOULIN, M.J., LABERGE, M., DE MARCELLIS, N. et PEIGNIER, I. (2002). Le risque : un modèle conceptuel d'intégration. Rapport de projet, Centre Interuniversitaire de recherche en Analyse des Organisations, Montréal, Québec, Canada, 66 p.

BEYELER, W. E., GLASS, R. J., BECH, M. and SORAMÄKI, K. (2006). Congestion and Cascades in Payment Systems. Federal Reserve Bank of New York, Staff Reports, Staff Report no. 259, September 2006, New-York, USA, 39 p. Site Internet du National Infrastructure Simulation and Analysis Center [En ligne], États-Unis.
http://www.ny.frb.org/research/staff_reports/sr259.html (Consulté le 5 août 2008).

BIER, V. M., HAIMES, Y. Y., LAMBERT, J. H., MATALAS, N. C. et ZIMMERMAN, R. (1999). A Survey of Approaches for Assessing and Managing the Risk of Extremes. Risk Analysis, Vol. 19, No. 1, pp. 83-94.

BLANCHER, P. (1998). Risques et réseaux techniques urbains. Ministère de l'Équipement, des Transports et du Logement. Centre d'études sur les réseaux, les transports, l'urbanisme et les constructions publiques. Collection du Certu, Lyon, France, 166 p.

BONNEVILLE, J.-P. (1999). Installations fixes d'extinction. Presses Internationales Polytechnique, Canada, 468 p.

BOURRELIER, P.-H., DENEUFBOURG, G. et DE VANSSAY, B. (2000). Les catastrophes naturelles, le grand cafouillage. Osman Eyrolles Santé & Société, France, 262 p.

BRUNSDON, D. R., DALY, M. C., and LAMB, A. J. W. (2003). Lifelines and earthquake: a review of New Zealand's key vulnerabilities. 7th Pacific conference on earthquake engineering, New Zealand society for earthquake engineering, Bulletin of the New Zealand society for earthquake engineering, 2003, Vol. 36, No. 2, pp. 146-154 [En ligne], New Zealand. https://db.nzsee.org.nz/PCEE/2003/Print/Paper146p.pdf (Consulté le 15 juillet 2008).

CAN\CSA (1997). Risk analysis requirements and guidelines: quality management. A national standard for Canada. Conseil canadien des normes, Association canadienne de normalisation, CAN-CSA Q850.

CCGU (2007a). Connaissance des infrastructures essentielles. Cours du Collège canadien de la gestion des urgences, 2 octobre 2007, École Polytechnique de Montréal, Québec, Canada.

CCGU (2007b). De l'évaluation de la vulnérabilité à la gestion des risques. Séminaire du Collège canadien de la gestion des urgences présenté par Benoît Robert et Rémi Beylot, 7 février 2007, Collège canadien de gestion des urgences, Ottawa, Ontario, Canada.

CCGU (2008). Étude des interdépendances entre les infrastructures essentielles. Atelier du Collège canadien de la gestion des urgences présenté par Benoît Robert, 10 mars 2008, Collège canadien de gestion des urgences, Ottawa, Ontario, Canada.

CHENG, Q. (2008). Emergency management using geographic decision support systems. Third Symposium on Joint infrastructure interdependencies research program (JIIRP), March 11, 2008, Ottawa, Ontario, Canada.

CLANCY, A. (2008). Domino effects & infrastructure resilience. Critical infrastructure workshop, Public Safety Canada, Friday, April 25, Ottawa, Ontario, Canada.

CLINTON, W. J. (1996). Executive order 13010 – Critical Infrastructure Protection. Presidential document, Federal Register, July 17, 1996, Vol. 61, No. 138, pp. 37345-37350.

CLUSIF (1997). MAGDA : Méthode d'Administration et de Gestion des Droits et Accréditations. Commission technique de sécurité logique, Club de la Sécurité des Systèmes d'Information Français, Paris, France, 47 p.

CLUSIF (1999). INCAS V2 : Intégration dans la Conception des Applications de la Sécurité. Commission qualité et sécurité des systèmes d'information, Club de la Sécurité des Systèmes d'Information Français, Paris, France, 59 p.

CLUSIF (2003). Méthode MEHARI. Site Internet du Club de la Sécurité des Systèmes d'Information Français [En ligne], France. https://www.clusif.asso.fr/fr/production/mehari/ (Consulté le 24 février 2004).

CNFSH (2003). Risque hydrologique ou lié à l'eau. Dictionnaire français d'hydrologie, Comité National Français des Sciences Hydrologiques, Commission de terminologie. Site Internet du centre des géosciences de l'École des Mines de Paris [En ligne], France. http://www.cig.ensmp.fr/~hubert/glu/FRDIC/DICRISQU.HTM (Consulté le 17 mars 2008).

COBB, A. (1997). Australia's vulnerability to information attacks. Australian Strategic and Defence Studies Centre, Australia.

COBB, A. (1999). Critical infrastructure attack: An investigation of the vulnerability of an OECD country. In Bosch, J.M.J., Luiijf, H.A.M., Mollema, A.M. (Eds.) NL ARMS – Netherlands Annual Review of Military Studies 1999: Information Operations, Tilburg University Press, Tilburg, Netherlands, pp. 201-222.

COHEN, P. (1986). Heuristic reasoning about uncertainty: an artificial intelligence approach. Pitman publishing limited, London, United-Kingdom, 204 p.

COMMISSION DES COMMUNAUTÉS EUROPÉENNES (2005). Livre vert sur un programme européen de protection des infrastructures critiques. COM(2005) 576 final, Bruxelles, Belgique, 28 p.

COMMISSION DES COMMUNAUTÉS EUROPÉENNES (2006a). Proposition de directive du conseil concernant le recensement et le classement des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. SEC(2006) 1648, SEC(2006) 1654 Bruxelles, Belgique, 30 p.

COMMISSION DES COMMUNAUTÉS EUROPÉENNES (2006b). Communication de la commission sur un programme européen de protection des infrastructures critiques. COM(2006) 786 final, Bruxelles, Belgique, 13 p.

COMMISSION DES COMMUNAUTÉS EUROPÉENNES (2006c). Document accompagnant la proposition de directive du conseil concernant le recensement et le classement des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Document de travail des services de la commission, Résumé de l'analyse d'impact, COM(2006) 787 final, SEC(2006) 1654, Bruxelles, Belgique, 8 p.

COMMISSION DES COMMUNAUTÉS EUROPÉENNES (2007). Appel à propositions 2007. Appel faisant suite à la décision de la Commission n° C(2006) 5025 du 26 octobre 2006 relative au financement d'un projet pilote comportant des actions préparatoires destiné à renforcer la lutte contre le terrorisme, Subvention à l'action, Site Internet de la Commission européenne [En ligne], Bruxelles, Belgique, 10 p.
http://ec.europa.eu/justice_home/funding/2004_2007/epcip/doc/call_2007_fr.pdf (Consulté le 31 juillet 2008).

CONRAD, S. H. and O'REILLY, G. P. (2006). An Overview of Energy and Telecommunications Interdependencies Modeling at NISAC. NATO Critical Infrastructure Workshop Proceedings, May 2006, 8 p. Site Internet du National Infrastructure Simulation and Analysis Center [En ligne], États-Unis.
http://www.sandia.gov/nisac/pub_papers.html (Consulté le 5 août 2008).

CONRAD, S. H., LECLAIRE, R. J., O'REILLY, G. P. and UZUNALIOGLU, H. (2006). Critical national infrastructure reliability modeling and analysis. Bell Labs Technical Journal, Vol. 11, No. 3, pp. 57-71.

CPNI (2008). Centre for the Protection of the National Infrastructure. Site Internet du Centre for the Protection of the National Infrastructure [En ligne], Grande-Bretagne.
http://www.cpni.gov.uk/ (Consulté le 31 juillet 2008).

CRAIM (2007). Guide de gestion des risques d'accidents industriels majeurs à l'intention des municipalités et de l'industrie. Conseil pour la réduction des accidents industriels majeurs, Montréal, Québec, Canada, 436 p.

CSIRO (2008). Protecting Australia's critical infrastructure with CIPMA. Commonwealth Scientific and Industrial Research Organisation, site Internet du Commonwealth Scientific and Industrial Research Organisation [En ligne], États-Unis.
http://www.csiro.au/partnerships/CIPMA.html (Consulté le 13 février 2008)

CSIS (2008). Securing cyberspace for the 44th presidency. A report of the CSIS Commission on Cybersecurity for the 44th presidency, Center for Strategic and International Studies, December 2008, Whashington, DC, États-Unis, 96 p.

DEHAIL, V. (2003). Défaillance d'un réseau de support à la vie : application de la logique floue dans l'évaluation des conséquences. Mémoire de maîtrise recherche, École Polytechnique de Montréal, Département des génies civil, géologique et des mines, Québec, Canada, 92 p.

DE LA LANDE DE CALAN, R. (2007). Modélisation des interdépendances pour identifier et anticiper les effets domino. Mémoire de maîtrise recherche, École Polytechnique de Montréal, Département de mathématiques et de génie industriel, Québec, Canada, 102 p.

DENIS, H. (1998). Comprendre et gérer les risques sociotechnologiques majeurs. Éditions de l'École Polytechnique de Montréal, Québec, Canada, 342 p.

DHS (2008). Protected Critical Infrastructure Information (PCII) Program. Site Internet du Department of Homeland Security [En ligne], États-Unis.
http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm (Consulté le 13 février 2008)

DICKINSON COLLEGE (2008). Three Mile Island Emergency. Site Internet du collège Dickinson [En ligne], États-Unis.
http://www.threemileisland.org/ (Consulté le 13 février 2008).

ÉDITEUR OFFICIEL DU QUÉBEC (2008). Loi sur la sécurité civile. L.R.Q., chapitre S-2.3. [En ligne], Québec, Canada. http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/S_2_3/S2_3.htm (Consulté le 13 février 2008)

EL-DIRABY, T. (2007). Developing a Model of Infrastructure Interdependencies. First Symposium on Joint infrastructure interdependencies research program (JIIRP), March 6, 2007, Ottawa, Ontario, Canada.

ELLISON, J. (2007). Modeling the US Natural Gas Network. Institute of Industrial Engineers (IIE) Transactions (2007) 39, 6 p. Site Internet du National Infrastructure Simulation and Analysis Center [En ligne], États-Unis. http://www.sandia.gov/nisac/pub_papers.html (Consulté le 5 août 2008).

EUROPA (2008). Programme européen de protection des infrastructures critiques. Site Internet de la Commission européenne [En ligne], Bruxelles Belgique. http://ec.europa.eu/justice_home/funding/epcip/funding_epcip_fr.htm (Consulté le 31 juillet 2008).

FACULTÉ POLYTECHNIQUE DE MONS (1998). Méthodologie pour l'identification et l'évaluation des effets domino. Ministère Fédéral de l'Emploi et du Travail, Administration de la sécurité du travail, Direction risques chimiques, Métatechnique, CRC/MT/003, première édition, 93 p.

FEMA (2002). World Trade Center, Building performance study: data collection, preliminary observations and recommendations. Federal Emergency Management Agency, Federal insurance and mitigation administration, Washington, DC, FEMA Region II, New York, pagination multiple.

GARIN, H. (1994). AMDEC/AMDE/AEEL : L'essentiel de la méthode. Association française de normalisation, France, 40 p.

GPNC (2000). Les infrastructures canadiennes et leurs interdépendances. Groupe de Planification Nationale des Contingences, Canada, 168 p.

GUICHARDET, G. (2009). Structuration et modélisation des connaissances nécessaires à l'évaluation des interdépendances entre les réseaux de support à la vie. Mémoire de maîtrise recherche, École Polytechnique de Montréal, Département de mathématiques et de génie industriel, Québec, Canada, 150 p.

GUILLAUME, F. (2005). Étude portant sur les vulnérabilités internes d'une usine de production d'eau potable. École des Mines d'Alès, stage effectué au *Centre risque & performance de l'École Polytechnique de Montréal*, École Polytechnique de Montréal, Département de mathématiques et de génie industriel, Québec, Canada pagination multiple.

HÉMOND, Y. (2008). Évaluation de la dépendance des réseaux de support à la vie face au réseau routier. Mémoire de maîtrise recherche, École Polytechnique de Montréal, Département de mathématiques et de génie industriel, Québec, Canada, 68 p.

HOME OFFICE (2008). Working together to protect the public. Site Internet du Home office [En ligne], Grande-Bretagne.
http://www.homeoffice.gov.uk/ (Consulté le 31 juillet 2008).

HUBERT G. et LEDOUX B. (1999). Le coût du risque. L'évaluation des impacts socio-économiques des inondations. Presses de l'École Nationale des Ponts et Chaussées, France, 232 p.

IBM (2008). Bonnes pratiques de sécurité SCADA. Site Internet de IBM [En ligne], France.
http://www-935.ibm.com/services/fr/index.wss/offering/gts/f1027203 (Consulté le 4 août 2008).

INDUSTRIAL DEFENDER (2008). Cyber Risk Protection. Site Internet d'Industrial Defender [En ligne], États-Unis. http://www.industrialdefender.com/ (Consulté le 4 août 2008).

INERIS (2003). Outils d'analyse des risques générés par une installation industrielle. Institut national de l'environnement industriel et des risques, Direction des risques accidentels, Formalisation du savoir et des outils dans le domaine des risques majeurs (DRA-35), Ω-7, France, 78 p.

INFRASTRUCTURE CANADA (2008). Les infrastructures essentielles nationales. Site Internet d'Infrastructure Canada [En ligne], Canada. http://www.infrastructure.gc.ca/research-recherche/result/wr-atr/decks/ocipep_f.shtml#11 (Consulté le 13 février 2008).

INHES (2008a). Gestion de crise. Site Internet de l'institut national des hautes études de sécurité [En ligne], France. http://www.inhes.interieur.gouv.fr/Gestion-de-crise-7.html (Consulté le 31 juillet 2008).

INHES (2008b). Appel à propositions de recherche – INHES 2008. Institut national des hautes études de sécurité. Site Internet de l'institut national des hautes études de sécurité [En ligne], France, 10 p. http://www.inhes.interieur.gouv.fr/fichiers/FER_AppelPropositions_2008.pdf (Consulté le 31 juillet 2008).

IPCC (2001). Climate Change 2001: The Scientific Basis. Contribution of Working Group I to the Third Assessment Report of the Intergovernmental Panel on Climate Change (IPCC). T. Houghton, Y. Ding, D.J. Griggs, M. Noguer, P. J. van der Linden and D. Xiaosu (Eds.) Cambridge University Press, UK., 944 p. Site Internet de l'Intergovernmental panel on climate change [En ligne], Suisse. http://www.ipcc.ch/pub/un/giecgt1.pdf (Consulté le 25 février 2004)

IRSN (2008). Les leçons de Tchernobyl. Institut de radioprotection et de sûreté nucléaire, site Internet de l'Institut de radioprotection et de sûreté nucléaire [En ligne], France. http://www.irsn.org/index.php?position=lecons_tchernobyl_accueil (Consulté le 13 février 2008).

JACOBSON, R. V. (2004). Operationnal risk management: theory and practice. Symposium on Risk Management and Cyber-Informatics: RMCI'04, July 18-21, Orlando, Florida, USA.

JOHNSON, P.-M., COUTURE, A. et NICOLET, R. (2007). Rapport de la commission d'enquête sur l'effondrement du viaduc de la Concorde. Gouvernement du Québec, site Internet de la commission d'enquête sur l'effondrement du viaduc de la Concorde [En ligne], Québec, Canada, 224 p. http://www.cevc.gouv.qc.ca/Rapport/index.html (Consulté le 15 novembre 2008)

KAPLAN, S. (1997). The world of risk analysis. Risk analysis, Vol. 17, pp. 407-417.

KERAVEL F. (1997). Fiabilité humaine et situation de travail, comprendre pour optimiser. Masson, collection des monographies de médecine du travail, France, 176 p.

KHAYATE, W. (2008). Étude de vulnérabilité d'une organisation en continuité des opérations. Mémoire de maîtrise recherche, École Polytechnique de Montréal, Département de mathématiques et de génie industriel, Québec, Canada, 91 p.

KRUTZ, R. L. (2006). Securing SCADA systems. John Wiley & Sons, Indianapolis, Etats-Unis, 238 p.

LALONDE, P.-L. (2005). La gestion de projets analysée selon la pragmatique communicationnelle de Paul Watzlawick. Mémoire de maîtrise recherche, École Polytechnique de Montréal, Département de mathématiques et de génie industriel, Québec, Canada, 183 p.

LANGLOIS, P. (1995). Introduction à la méta-sécurité. Planète Internet. Site Internet Intrinseq Business continuity and security [En ligne], France. http://www.intrinsec.com/articles/articles/sept95_planete_internet.htm (Consulté le 15 novembre 2003).

LAPOINTE, M. (2006). Gestion d'urgences dédiée à la communication de crise. Présentation de Marc Lapointe, chef divisionnaire sûreté à Bell Canada dans le cadre du cours CIV6214, Gestion des catastrophes, Département des Génies civil, géologique et des mines, École polytechnique de Montréal, Québec, Canada.

LASBORDES, P. (2006). La sécurité des systèmes d'information : un enjeu majeur pour la France. La documentation française, collection des rapports officiels, Paris, France, 200 p.

LEDROIT (2008). Cyber-attaques contre Tbilissi. Journal LeDroit, mercredi 13 août 2008, Québec, Canada, p. 22.

LEMOIGNE, J.-L. (1990). Systémique et complexité : études d'épistémologie systémique. Revue Internationale de Systémique, Vol. 4, No°2, pp. 107-117.

LEMONDE (2008). La crise en questions. Site Internet du Journal LeMonde [En ligne], France. http://www.lemonde.fr/economie/article/2008/09/16/la-crise-financiere-en-questions_1095762_3234.html (Consulté le 7 décembre 2008).

LEYDEN, J. (2008). Polish teen derails tram after hacking train network. Site Internet The register [En ligne], Grande-Bretagne. http://www.theregister.co.uk/2008/01/11/tram_hack/ (Consulté le 1 août 2003).

LESECHOS (2008). La crise financière mondiale au jour le jour. Site Internet du Journal LesEchos [En ligne], France. http://www.lesechos.fr/info/finance/300293082-la-crise-financiere-mondiale-au-jour-le-jour.htm (Consulté le 7 décembre 2008).

LETEMPS (2008). Le Japon s'installe dans la récession. Site Internet du Journal LeTemps [En ligne], Suisse. http://www.letemps.ch/template/transmettre.asp?contenupage=nlreader&page=newsletterdisplay&id=14&NLArtID=15369 (Consulté le 7 décembre 2008).

LONDON RESILIENCE TEAM (2008). London Strategic Emergency Plan. Site Internet de la London Resilience Team [En ligne], Grande-Bretagne. http://www.londonprepared.gov.uk/londonsplans/ (Consulté le 31 juillet 2008).

LUIIJF, E.; BURGER, H. and KLAVER, M. (2003). Critical Infrastructure Protection in the Netherlands: A Quick-scan. In U.E. Gattiker (Ed.), EICAR Conference Best Paper Proceedings, Copenhagen, Danemark, 19 p.

MARTI, J., JUAREZ-GARCIA, H. and VENTURA, C. (2008). Critical linkages to infrastructure networks. Third Symposium on Joint infrastructure interdependencies research program (JIIRP), March 11, 2008, Ottawa, Ontario, Canada.

MCBEAN, E. and SCHUSTER, C. (2008). Resilience of water infrastructure and health response systems against waterborne diseases. Third Symposium on Joint infrastructure interdependencies research program (JIIRP), March 11, 2008, Ottawa, Ontario, Canada.

MCGREGOR, W. S. (2007). Willows man arrested for hacking into Tehama Colusa Canal Authority computer system. News release, Department of justice, United States Attorney, Eastern District of California, 2 p. Site Internet du United States Department of Justice [En ligne], États-Unis. http://www.usdoj.gov/usao/cae/press_releases/docs/2007/11-28-07KeehnInd.pdf (Consulté le 1 août 2008).

MEEDA (2008a). La directive Seveso : pour une prévention des risques majeurs. Site Internet du Ministère de l'Écologie, de l'Énergie, du Développement durable et de l'Aménagement du territoire [En ligne], France. http://www.ecologie.gouv.fr/La-directive-SEVESO-Pour-une.html (Consulté le 31 juillet 2008).

MEEDA (2008b). Liste et définition des risques majeurs. Ministère de l'écologie, de l'énergie, du développement durable et de l'aménagement du territoire. Site Internet du portail de la prévention des risques majeurs, Prim.net [En ligne], France. http://www.prim.net/ (Consulté le 17 mars 2008)

MIBS (2006). Les infrastructures critiques : bien maîtriser le socle du patrimoine informatique de l'entreprise. Livre blanc, MIBS Infrastructure & Services, 23 p.

MILI, L., QIU, Q. and PHADKE, A. G. (2004). Risk assessment of catastrophic failures in electric power systems. International Journal of critical infrastructures, Vol. 1, No. 1, pp. 38-63.

MINISTÈRE FÉDÉRAL DE L'EMPLOI ET DU TRAVAIL (2000). Réglementation sur la directive SEVESO II : Direction des risques chimiques. Inspection technique de l'administration de la sécurité du travail du Ministère Fédéral de l'Emploi et du Travail. Site Internet du Service public fédéral Emploi, Travail et Concertation [En ligne], Belgique. http://meta.fgov.be/pm/pmc/frmc17.htm (Consulté le 15 novembre 2003).

MODARRES, M., KAMINSKY, M. and KRIVTSOV, V. (1999). Reliability engineering and risk analysis, a practical guide. Marcel Dekker, Quality and reliability, 542 p.

MSP (2007a). Cadre de référence pour la gestion des risques, Direction générale de la sécurité civile et de la sécurité incendie, document de consultation. Ministère de la sécurité publique du Québec, Québec, Canada, 34 p.

NEAULT, J.-M. (2009). La résilience des systèmes essentiels au Québec. Résilience, Bulletin d'information en sécurité civile du ministère de la Sécurité publique, Québec, Hiver-Printemps 2009, Vol. 4, No. 1, pp. 4-5.

NICOLET, J. L. et CELIER, J. (1985). La fiabilité humaine dans l'entreprise. Collection le nouvel ordre économique, Masson, France, 302 p.

NICOLET, R., TRUDEAU, N., DENIS, H., BERNIER, C., CLOUTIER, L., DICAIRE, A. et ROY, A. (1999). Pour affronter l'imprévisible : les enseignements du verglas de 1998. Rapport de la commission scientifique et technique chargée d'analyser les événements relatifs à la tempête de verglas survenue du 5 au 9 janvier 1998. Les Publications du Québec, Gouvernement du Québec, Québec, Canada, 442 p.

NISAC (2003). National Infrastructure Simulation and Analysis Center. Site Internet du Sandia National Laboratories [En ligne], États-Unis. http://www.sandia.gov/CIS/ (Consulté le 20 février 2004)

OCDE (2003). La formation des ingénieurs en matière de gestion des risques. Conférence sur la formation des ingénieurs en matière de gestion des risques. Organisation de Coopération et de Développement Économique, 21 au 24 octobre 2003, Montréal, Québec, Canada.

OEA (2002). 21 Steps to Improve Cyber Security of SCADA Networks. The President's Critical Infrastructure Protection Board, Office of Energy Assurance, U.S. Department of Energy, USA, 10 p. Site Internet de l'United States Department of Energy [En ligne], États-Unis. http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf (Consulté le 5 août 2008).

OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE (2008). Définition du mot cybernétique. Site Internet du grand dictionnaire terminologique [En ligne], Québec, Canada. http://w3.granddictionnaire.com/btml/fra/r_motclef/index1024_1.asp (Consulté le 15 juillet 2008).

OSCQ (2008). Exercice Domino : résilience des systèmes essentiels. Atelier de travail de l'Organisation de sécurité civile du Québec, 13 novembre 2008, Québec, Québec, Canada.

OTAN (2007). La protection des infrastructures critiques. Assemblée parlementaire de l'Organisation du traité de l'atlantique nord, 162 CDS 07 F rév. 1. Site Internet de l'organisation du traité de l'atlantique nord [En ligne]. http://www.nato-pa.int/default.asp?CAT2=1159&CAT1=16&CAT0=2&COM=1165&MOD=0&SMD=0&SSMD=0&STA=&ID=0&PAR=0&LNG=1 (Consulté le 31 juillet 2008).

PAGEON, J. (2008). Méthodologie d'évaluation de la vulnérabilité d'une MRC face aux ressources essentielles. Mémoire de maîtrise recherche, École Polytechnique de Montréal, Département de mathématiques et de génie industriel, Québec, Canada, 94 p.

PAPADEMOS, L. D. (2007). Avis de la banque centrale européenne du 13 avril 2007. Journal officiel de l'Union européenne, Con/2007/11, 2007/C116/01, 2 p.

PEDERSON, P., DUDENHOEFFER, D. HARTLEY, S. and PERMANN, M. (2006). Critical Infrastructure Interdependency Modeling: A survey of U.S. and International Research. Idaho National Laboratory, USA, 132 p.

PEERENBOOM, J. and FISHER, R. (2007). Interdependencies – Understanding the linkages. Atelier sur les travaux du Argonne National Laboratory, Collège Canadien de Gestion des Urgences, 16 novembre 2007, Ottawa, Ontario, Canada.

PETIT, F. (2003). Erreur humaine : Évaluation des possibilités d'apparition et intégration dans les causes de nature anthropique. Rapport de projet présenté dans le cadre du programme de maîtrise en génie civil, Département des génies civil, géologique et des mines, École Polytechnique de Montréal, Québec, Canada, 103 p.

PETIT, F. et ROBERT, B. (2004). How can analysis of human reliability help to improve cyber security? Symposium on risk management and cyber-informatics (RMCI'04), The 8th World Multi-Conference on Systemics, Cybernetics and Informatics, Proceeding 2004, Volume XV, July 18-21, Orlando, Florida, USA, pp. 335-339.

PETIT, F. et ROBERT, B. (2007). La vulnérabilité cybernétique des infrastructures essentielles. Symposium national sur les télécommunications d'urgence, 25-26 septembre, Montréal, Québec, Canada.

PETIT, F., ROBERT, B. et ROUSSELLE, J. (2004). Une nouvelle approche pour la caractérisation des aléas et l'évaluation des vulnérabilités des réseaux de support à la vie. Revue Canadienne de Génie Civil, No. 31, pp. 333-344.

PR NEWSWIRE (2008). Verano élargit son réseau mondial de distribution pour Industrial Defender(R) [En ligne], Grande-Bretagne. http://www.prnewswire.co.uk/cgi/news/release?id=181693 (Consulté le 4 août 2008).

PROJECT MANAGEMENT INSTITUE (2008). A guide to the Project management body of knowledge (Pmbok guide), fourth edition. Project Management Institute, Newtown Square, Pa, 388 p.

QUACH, T.T., GAGNON, J., ROBERT, B. et MARCHE, C. (2000). Upper Ottawa River: A Four Step Risk Assessment. 20th Congress, International Commission on Large Dams, Q76-R32, 19-20 September, Beijing, China, pp. 479-498.

RADIO CANADA (2008). Royaume-Uni, L'échec de la vidéosurveillance. Site Internet de Radio Canada [En ligne], Canada. http://www.radio-canada.ca/nouvelles/International/2008/05/06/004-cameras_uk.shtml (consulté le 31 juillet 2008).

RDDC (2009). Modèle d'évaluation consolidée des risques. Programme technique de sécurité publique. Site Internet de Recherche et développement pour la défense Canada [En ligne], Canada. http://www.css.drdc-rddc.gc.ca/pstp/priorities-priorites/risk-risques-fra.asp (consulté le 20 avril 2009).

REASON J. (1993). L'erreur humaine. Traduction française de Human error effectuée par Jean-michel hoc, Presses universitaires de France, collection le travail humain, 366 p.

REASON, J. (2000). Human error: models and management. British medical journal, Vol. 320, pp. 768-770.

REDMAN, T. (1998). La qualité des données à l'âge de l'information. Artech House Inc., Masson, Paris, France, 264 p.

RINALDI, S. M., PEERENBOOM, J. P. and KELLY, T. K. (2001). Identifying, understanding and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, Vol. 21, No. 6, pp. 11-25.

RNC (2008). Éléments naturels – Leçons tirées de la panne d'électricité de 2003. Ressources naturelles Canada, site Internet de Ressources naturelles Canada [En ligne], Canada. http://www.nrcan.gc.ca/com/elements/issues/11/blapan-fra.php (Consulté le 13 février 2008).

ROBERT, B. (1989). Un système expert d'aide à la conception hydraulique. Thèse de Philosophiae Doctor, École Polytechnique de Montréal, Département de Génie civil, 222 p.

ROBERT, B. (2001). A Method for the Study of Cascading Effects Within Lifeline Networks. Workshop on Mitigating the Vulnerability of Critical Infrastructures to Catastrophic Failures, September 10-11, Alexandria, USA.

ROBERT, B. (2008). Méthodologie d'étude des interdépendances entre les réseaux de support à la vie. Troisième Symposium sur le Programme conjoint de recherche sur les interdépendances relatives aux infrastructures (PCRII), 11 mars 2008, Ottawa, Ontario, Canada.

ROBERT, B. and CLOUTIER, I. (2007). Geoinformation for Risk Prevention – The Challenges Facing Critical Infrastructure Protection. Joint CIG/ISPRS Conference on Geomatics for Disaster and Risk Management, May 22–25, Toronto, Ontario, Canada.

ROBERT, B. and MORABITO, L. (2008). The operational tools for managing physical interdependencies among critical infrastructures. International Journal of Critical Infrastructures, Vol. 4, No. 4, pp. 353–367.

ROBERT, B. et MORABITO, L. (2009). Réduction de la vulnérabilité des infrastructures essentielles face à leurs interdépendances : Guide méthodologique. Éditions Tec & Doc, collection Sciences du risque et du danger, Lavoisier, 80 p.

ROBERT, B. et PETIT, F. (2006). Vulnérabilité d'une municipalité aux inondations : une approche par conséquences. Congrès annuel 2006 de l'Association Canadienne des Barrages, 30 sept.-5 oct., Québec, Québec, Canada.

ROBERT, B., SENAY, M.-H., PLAMONDON, M.-E. et SABOURIN, J.-P. (2003a). Caractérisation et hiérarchisation des liens reliant des réseaux de support à la vie. Projet CDT P2800. Bureau de la Protection des Infrastructures Essentielles et de la Protection Civile, Canada, 70 p.

ROBERT, B., SABOURIN, J.-P., GLAUS, M., PETIT, F. et SENAY, M.-H. (2003b). A New Structural Approach for the study of Domino Effects Between Life Support Networks. Building Safer Cities: The Future of Disaster Risk. Washington, D. C., Provention Consortium, The World Bank, pp. 245-272.

ROBERT, B., PETIT, F., and RICCIARDI-RIGAULT, M. (2004a). A new approach to evaluate life support network vulnerabilities. 14th World Conference on Disaster Management, June 20-23, Toronto, Ontario, Canada.

ROBERT, B., PETIT, F., SENAY, M.-H. et SABOURIN J.-P. (2004b). Modélisation des transferts de vulnérabilités entre des réseaux de support à la vie. Bureau de la Protection des Infrastructures Essentielles et de la Protection Civile, Rapport final, 57 p.

ROBERT, B., MARCHE, C., ROUSSELLE, J. and PETIT, F. (2006). Method for consequence curves - as applied to flood risks. International Journal of Emergency Management, Vol. 3, Nos. 2/3, pp. 192-214

ROBERT, B., MORABITO, L. and QUENNEVILLE, O. (2007). The preventive approach to risks related to interdependent infrastructures. International Journal of Emergency Management, Vol. 4, No. 2, pp. 166–182.

ROBERT, B., DE CALAN, R. and MORABITO, L. (2008). Modelling interdependencies among critical infrastructures. International Journal of Critical Infrastructures, Vol. 4, No. 4, pp. 392–408.

SCOTT, G. (2007). CIPMA – Critical Infrastructure Protection Modelling and Analysis : Overview of CIP in Australia. Séminaire technologique du *Centre risque & performance*, 15 novembre 2007, École Polytechnique de Montréal, Québec, Canada.

SÉCURITÉ SCADA (2008). Sécurité des systèmes SCADA. Site Internet de Sécurité SCADA [En ligne], France.
http://scadable.com/ (Consulté le 5 août 2008).

SÉCURITÉ PUBLIQUE QUÉBEC (2008). Les mécanismes de coordination de l'intervention gouvernementale. Site Internet de Sécurité publique Québec [En ligne], Québec, Canada.
http://www.msp.gouv.qc.ca/secivile/secivile.asp?txtSection=apercu&txtCategorie=coordination (Consulté le 15 novembre 2008).

SEIDOU, O. (2002). Intégration du risque dans les modes de gestion des systèmes hydriques. Philosophiae Doctor Thesis (Ph.D.), École Polytechnique de Montréal, Département des génies civil, géologique et des mines, Québec, Canada, 251 p.

SLAY, J. and MILLER, M. (2008). Lessons learned from the Maroochy water breach. Critical infrastructure protection, chapter 6, pp. 70-82. Site Internet du World computer Congress 2008 [En ligne], Milan, Italie.
http://www.wcc2008.org/site/IFIPSampleChapter.pdf (Consulté le 1 août 2008).

SNC-LAVALIN (2006). Implantation d'un terminal méthanier à Lévis, Étude d'impacts sur l'environnement. Tome 3, Terminal méthanier, Volume 1 : Rapport principal, 366 p.

SNL (2008). Cyber security. Site Internet du Sandia National Laboratories [En ligne], États-Unis.
http://www.sandia.gov/mission/homeland/programs/cyber/index.html (Consulté le 13 février 2008).

SORAMÄKI, K., BECH, M. L., ARNOLD, J., GLASS, R. J. and BEYELER, W. E. (2007). The Topology of Interbank Payment Flows. Physica A 379 (2007), ScienceDirect, Elsevier, pp. 317–333.

SPC (2007). Un cadre de sécurité civile pour le Canada. Direction générale des politiques de gestion des urgences, Sécurité publique et Protection civile Canada, 16 p, Site Internet de Sécurité publique Canada [En ligne], Canada.
http://www.securitepublique.gc.ca/prg/em/_fl/emfrmwrk-fr.pdf (Consulté le 22 avril 2008)

SPC (2008a). Protéger une société ouverte : la politique canadienne de sécurité nationale. Site Internet de Sécurité publique Canada [En ligne], Canada.
http://www.securitepublique.gc.ca/pol/ns/secpol04-fra.aspx (Consulté le 31 juillet 2008).

SPC (2008b). Protection des infrastructures essentielles. Site Internet de Sécurité publique Canada [En ligne], Canada.
http://www.securitepublique.gc.ca/prg/em/cip-fra.aspx (Consulté le 31 juillet 2008).

SPC (2008c). Aller de l'avant avec la Stratégie nationale sur les infrastructures essentielles : Stratégie (Partie 1). Site Internet de Sécurité publique Canada [En ligne], Canada.
http://www.securitepublique.gc.ca/prg/em/cip/strat-part1-fra.aspx (Consulté le 31 juillet 2008).

SPC (2008d). Aller de l'avant avec la Stratégie nationale sur les infrastructures essentielles : Plan d'action (Partie 2). Site Internet de Sécurité publique Canada [En ligne], Canada.
http://www.securitepublique.gc.ca/prg/em/cip/strat-part2-fra.aspx (Consulté le 31 juillet 2008).

SPC (2008e). Programme conjoint de recherché sur les interdépendances des infrastructures. Site Internet de Sécurité publique Canada [En ligne], Canada.
http://www.securitepublique.gc.ca/prg/em/jiirp/index-fra.aspx (Consulté le 25 février 2008).

SPC (2008f). Centre canadien de réponse aux incidents cybernétiques. Site Internet de Sécurité publique Canada [En ligne], Canada.
http://www.publicsafety.gc.ca/prg/em/ccirc/index-fra.aspx (Consulté le 25 février 2008).

STAMPF, N. (2002). La méthode MARION. Site Internet de Teamlog [en ligne], France.
http://www.securite.teamlog.com/publication/4/5/164/ (Consulté le 23 février 2004).

STEDINGER, J. R., HEATH, D.C. and THOMPSON, K. (1996). Risk analysis for dam safety evaluation: hydrologic risk. Institute of Water Resources, Report No. 96-13-16, 51 p.

TASSINARI, R. (2003). Pratique de l'analyse fonctionnelle, troisième édition. L'usine nouvelle, Dunod, Paris, France, 177 p.

TISN (2008). Critical infrastructure protection project. Site Internet du Trusted Information Sharing Network for critical infrastructure protection [En ligne], Australie.
http://www.offi.gov.au/agd/WWW/TISNHome.nsf/Page/CIP_Projects (Consulté le 13 février 2008).

TRUDEL, J. (2008). La cyberguerre mondiale a commencé. Journal L'Actualité, 1er décembre 2008, Québec, Canada, pp. 35-43.

UIT-T (2005). Qualité de service et qualité de fonctionnement du réseau. Manuel de l'Union internationale des télécommunications, Secteur de normalisation des télécommunications de l'UIT, Genève, Suisse, 118 p.

VANDERHAEGEN, F. (2003). Analyse et contrôle de l'erreur humaine. Hermes science publications, France, 214 p.

VIELLARD, L. et RIBNIKAR, D. (2003). La protection des infrastructures critiques face aux menaces asymétriques – Synthèse. Compagnie européenne d'intelligence stratégique, 6 p.

WEICHSELGARNER, J. (2001). Disaster mitigation: the concept of vulnerability revisited. Disaster Prevention and Management, Vol. 10, No. 2, pp. 85-94.

ZADEH, L. A. (1965). Fuzzy sets. Information and control, No°8, pp. 338-353.

ZHANG, W. (2008). Simulation of critical infrastructure networks. Third Symposium on Joint infrastructure interdependencies research program (JIIRP), March 11, 2008, Ottawa, Ontario, Canada.

ZIELINSKI, P. A. (2001). Flood frequency analysis in dam safety assessment. Proceedings of CDA annual conference, October, Fredericton, Canada, pp. 79-86.

ANNEXE

Annexe 1 - Comparaison entre les approches d'analyse des interdépendances entre infrastructures essentielles.

Pays - Région	AUSTRALIE		CANADA			ETATS-UNIS		EUROPE	
Nom	Attorney-General Department, Australia Commonwealth Scientific and Industrial Research Organisation (CSIRO)	Australian Government Computer Emergency Readiness Team	Groupe de Planification annuelle des Communications (GPAC)	Infrastructure interdependencies Simulation Team (I2SIM) Université de Colombie-Britannique	Centre risque & performance (CERP) Ecole Polytechnique de Montréal	National Infrastructure Simulation and Analysis Center (NISAC) Department of Homeland Security Preparedness Directorate	Argonne National Laboratory-Infrastructure Assurance Center	Centre for the Protection of National Infrastructure (CPNI) (Grande-Bretagne) France Pays-Bas	Union européenne
Programme	Critical infrastructure protection modelling and analysis program (CIPMA)	Computer network vulnerability assessment program (CNVA)		Programme conjoint de recherche sur les interdépendances des infrastructures (PCRII)		Modélisation des interdépendances, analyse des conséquences	Analyse des risques, analyse des interdépendances entre IE	CONTEST, livre blanc, Brainstorming vitale infrastructure, etc.	Programme européen de protection des infrastructures critiques (PEPIC)
Mandat - Objectifs -	Analyses et modèles de dépendances en réseaux d'IE	Etude des vulnérabilités et des corrélations reliées aux IE	Produire une évaluation des risques pour les infrastructures nationales	Caractériser les interdépendances entre IE	Caractériser les interdépendances entre IE, évaluer les effets domino entre IE	Forums des modèles et des simulations adaptés à l'analyse des IE, de leurs interdépendances et de leurs vulnérabilités	Forums des services et experts des organisations non publiques que parmi intervenants dans les domaines des mesures d'urgence associées aux IE	Protéger les IE	Protéger les IE

Annexe 1 - Comparaison entre les approches d'analyse des interdépendances entre infrastructures essentielles (suite).

Pays - Région	AUSTRALIE		CANADA			ETATS-UNIS		EUROPE	
Approche	Stratégique - Opérationnelle	Stratégique - Opérationnelle	Stratégique	Opérationnelle	Opérationnelle	Stratégique - Opérationnelle	Stratégique - Opérationnelle	Stratégique - Opérationnelle	Stratégique
Niveau d'analyse, d'implantation	National	National	National	Local	Local	National - local	National - local	National	International
Risques pris en compte	Analyse tous risques	Risque informatique	Liens de dépendance	Analyse tous risques	Analyse tous risques	Analyse tous risques Economiques	Analyse tous risques	Analyse tous risques Terrorisme	Analyse tous risques Terrorisme
Infrastructures essentielles considérées	Energie, finances, télécom.	Technologies de l'information, télécom.	Télécom., énergie, nucléaire, transports, alimentation, santé, services gouvernementaux	Télécom., énergie, eau, transports, gouvernement	Télécom., Energie, Transports, gouvernement (municipal, provincial et municipal), eau	Energie, finances, télécom.	Energie principalement	Energie électrique, télécom., transports, finances, santé, eau	Energie, industrie nucléaire, technologies de l'information et des communications, eau, alimentation, santé, finance, transports, industrie chimique, espace, installations de recherche

Annexe 1 - Comparaison entre les approches d'analyse des interdépendances entre infrastructures essentielles (suite).

Pays - Région	AUSTRALIE		CANADA			ETATS-UNIS		EUROPE	
Méthodes d'analyse de risque	Inductives basées sur des scénarios d'état	Inductives basées sur des scénarios	Inductives basées sur des scénarios	Inductives basées sur des scénarios	Déductives centrées sur les conséquences	Inductives et déductives basées sur des scénarios	Inductives basées sur des scénarios	Inductives basées sur des scénarios	Inductives basées sur des scénarios
Mise en œuvre - Outils	Modélisation géométrique à grande échelle	Indéterminé	Matrice de dépendances entre IE	Simulation informatique, systèmes d'information géographique	Matrices, courbes de dépendances, courbes de conséquences	Simulation informatique	Systèmes d'information géographique, outils de visualisation en 3D des IE	En développement	En développement
Développement d'un cadre d'échange d'informations	Oui Trusted Information Sharing Network (TISN)	Oui Trusted Information Sharing Network (TISN)	Non		Oui Espace de coopération	Oui Protection Critical Infrastructure Information par le Department of Homeland security Critical Infrastructure Protection Decision Support System (CIP/DSS)		En développement	Critical Infrastructure Warning Information Network (CIWIN)
Prise en compte de l'élément cybernétique	Non	Oui Sécurité informatique	Oui Dépendance face aux réseaux	Non	Non	Oui Sécurité informatique	Oui Sécurité informatique	Oui Sécurité informatique	Oui Sécurité informatique
Prise en compte de la fiabilité humaine	Non	Non	Non	Non	Oui Humain considéré comme une ressource	Non	Non	Non	Non